



AirCheck™

Wi-Fi Tester

Mode d'emploi

January 2010, Rev. 2 4/11 (French)

©2010-2011 Fluke Corporation. All rights reserved.

All product names are trademarks of their respective companies.

Wi-Fi® is a registered trademark of the WiFi Alliance.

EXCLUSION DE GARANTIE ET RESPONSABILITE LIMITEE

La société Fluke Networks garantit l'absence de vices de matériaux et de fabrication de ses produits dans des conditions normales d'utilisation et d'entretien. La période de garantie pour le testeur est de un an et prend effet à la date d'achat. Les pièces, les accessoires, le dépannage et l'entretien sont couverts par la garantie pour une période de 90 jours, sauf stipulation contraire. Les batteries lithium-ion, nickel-cadmium et nickel-métal-hydrure, les câbles ainsi que les autres produits périphériques sont considérés comme des pièces ou des accessoires. Cette garantie ne s'applique qu'à l'acheteur d'origine ou à l'utilisateur final s'il est client d'un distributeur agréé par Fluke Networks. Elle ne s'applique pas à tout produit qui, de l'avis de Fluke, a été malmené, modifié, négligé, contaminé ou endommagé par accident ou soumis à des conditions anormales d'utilisation et de manipulation. Fluke Networks garantit que le logiciel fonctionnera en grande partie selon ses spécifications fonctionnelles pendant une période de 90 jours et qu'il a été correctement enregistré sur des supports non défectueux. Fluke Networks ne garantit pas que le logiciel est exempt d'erreurs ou qu'il fonctionne sans interruption.

Les distributeurs agréés par Fluke Networks appliquent cette garantie à des produits neufs et qui n'ont pas servi, vendus à des utilisateurs finaux, mais ne sont pas autorisés à offrir une garantie plus étendue ou différente au nom de Fluke Networks. Le service de garantie est offert uniquement si le produit a été acheté à un point de vente agréé par Fluke Networks ou si l'acheteur a payé le prix international applicable. Fluke Networks se réserve le droit de facturer à l'acheteur les frais d'importation des pièces de réparation ou de remplacement si le produit acheté dans un pays a été expédié dans un autre pays pour y être réparé.

L'obligation de garantie de Fluke Networks est limitée, au choix de Fluke Networks, au remboursement du prix d'achat, ou à la réparation/remplacement gratuit du produit défectueux retourné dans le délai de garantie à un centre de service agréé par Fluke Networks.

Pour avoir recours au service de la garantie, mettez-vous en rapport avec le centre de service agréé Fluke Networks le plus proche afin de recevoir les références d'autorisation de renvoi, ou envoyez le produit accompagné d'une description du problème, port et assurance payés (franco lieu de destination), à ce centre de service. Fluke Networks n'assume aucune responsabilité en cas de dommages survenus au cours du transport. Après une réparation sous garantie, le produit sera retourné à l'acheteur, en port payé (franco lieu de destination). Si Fluke Networks estime que le problème a été causé par une négligence, un mauvais traitement, une contamination, une modification, un accident ou des conditions de fonctionnement ou de manipulation anormales, ou par une usure normale des composants mécaniques, Fluke Networks fournira un devis des frais de réparation et ne commencera la réparation qu'après en avoir reçu l'autorisation. Après la réparation, le produit sera renvoyé à l'acheteur, en port payé (franco point d'expédition) et les frais de réparation et de transport lui seront facturés.

LA PRESENTE GARANTIE EST LE SEUL ET EXCLUSIF RECOURS DE L'ACHETEUR ET TIENT LIEU DE TOUTES AUTRES GARANTIES, EXPRESSES OU IMPLICITES, Y COMPRIS, MAIS NON EXCLUSIVEMENT, TOUTE GARANTIE IMPLICITE DE VALEUR MARCHANDE OU D'ADEQUATION A UN USAGE PARTICULIER. FLUKE NETWORKS NE POURRA ETRE TENU RESPONSABLE D'AUCUN DOMMAGE OU PERTE PARTICULIER, INDIRECT, ACCIDENTEL OU CONSÉCUTIF, Y COMPRIS LES PERTES DE DONNÉES, SUR UNE BASE CONTRACTUELLE, EXTRA-CONTRACTUELLE OU AUTRE.

Etant donné que certains pays ou états n'admettent pas les limitations d'une condition de garantie implicite, ou l'exclusion ou la limitation de dégâts accidentels ou consécutifs, il se peut que les limitations et les exclusions de cette garantie ne s'appliquent pas à chaque acheteur. Si une disposition quelconque de cette garantie est jugée non valable ou inapplicable par un tribunal ou un autre pouvoir décisionnel compétent, une telle décision n'affecte en rien la validité ou le caractère exécutoire de toute autre disposition.

Table des matières

Titre	Page
Introduction	1
Enregistrement de votre produit	1
La base de connaissances de Fluke Networks	1
Pour contacter Fluke Networks	2
Informations sur la sécurité	2
Déballage	3
Testeur Wi-Fi AirCheck	3
Kit de dépannage de première ligne AirCheck	3
Caractéristiques physiques	4
Charge et durée de vie de la batterie	6
Configuration minimum pour des performances optimales	7
Informations fournies sur un réseau	8
Composition du réseau LAN sans fil	8
Connectivité des périphériques au réseau	9
Causes des ralentissements de performances réseau et des pertes de connexion	10
Sécurité du réseau	11
Réseaux ou points d'accès disponibles lorsque je me déplace	12
Consignation de l'état du réseau et de la session de test	12
Localisation d'un point d'accès	12

L'écran d'accueil	13
Configuration du testeur	14
Changer les paramètres linguistiques et nationaux	14
Créer un profil pour se connecter à des réseaux sécurisés	14
Paramètres	16
Fonctionnement 802.11d	20
Modifier les seuils des couleurs dans les affichages incrémentaux	21
Donner un état d'autorisation aux points d'accès	22
Détection des réseaux et des points d'accès	23
Si le testeur ne découvre pas de point d'accès	34
Remarques sur les réseaux et les points d'accès	35
Utilisation du canal	38
Vérification de la connectivité	41
Charger un profil qui comprend des identifiants de sécurité	42
Se connecter à un réseau ou à un point d'accès	42
Déte�ter un périphérique ou un serveur Web par commande ping	46
Détection des clients	49
Si le testeur ne détecte pas de client	54
Localisation d'un point d'accès ou d'un client	54
L'antenne directionnelle externe	58
R�glage des mesures d'intensit� du signal en fonction des autres p�riph�riques	61
Enregistrement d'une session de tests	62
Gestion des fichiers sur le testeur	63
A propos des fichiers sur le testeur	64
Transf�rer les fichiers vers un PC	65
Entretien	66
Nettoyer le testeur	66
Mettre � jour le logiciel dans le testeur	66

Restaurer aux réglages d'usine	67
Informations sur le périphérique	67
Si le testeur ne s'éteint pas	68
Options et accessoires	68
Caractéristiques techniques	69
Caractéristiques ambiantes	69
Caractéristiques générales	71
Caractéristiques de l'accès sans fil	72
Déclaration sur les interférences de la Federal Communication Commission des Etats-Unis et de Industrie Canada ...	75
Remarque importante : Déclaration FCC et IC sur l'exposition aux rayonnements	75
Déclaration de conformité de l'Union européenne (UE)	76
Annexe A : Messages du journal des échecs de connexion	79
Annexe B : Paramètres par défaut	83
Annexe C : 802.11d Codes de pays	85
Indice	95

Liste des figures

Figure	Page
1. Caractéristiques physiques	4
2. Comment retirer la batterie	6
3. L'écran d'accueil	13
4. Modifier les seuils des couleurs dans un affichage incrémental	21
5. Liste des réseaux (SSID)	24
6. Liste des points d'accès	28
7. Ecran Détails du point d'accès	32
8. Ecran Utilisation du canal	38
9. Ecran Détails util. canal	40
10. L'écran Connexion	44
11. Journal de connexion	45
12. L'écran Ping	47
13. Ecran Clients	50
14. Ecran Détails du client	52
15. Ecran Localiser point d'accès	55
16. Ecran Emplacement du client	56
17. Schéma de recherche de l'antenne omnidirectionnelle dans le testeur	57
18. Schéma de recherche de l'antenne externe	59
19. Comment orienter l'antenne externe	60
20. Schémas de l'antenne externe (magnitude (dBi)) ou azimut (degrés)	74

AirCheck™ Wi-Fi Tester

Introduction

Le testeur Wi-Fi AirCheck™ permet de vérifier que les réseaux locaux (LAN) sans fil 802.11 sont accessibles aux utilisateurs de téléphonie portable, d'examiner le taux d'utilisation des canaux pour mieux analyser l'intégrité du réseau et d'identifier la source des anomalies de connexion. Le testeur fonctionne sur les réseaux 802.11 b/g/n dans la bande 2,4 GHz et sur les réseaux 802.11 a/n dans la bande 5 GHz.

Le détecteur optionnel PoE indique si la tension PoE (Power over Ethernet) des dispositifs 802.3af et des dispositifs de puissance supérieure 802.3at est disponible sur les câbles de réseau à paire torsadée.

Vous pouvez enregistrer les résultats de test et utiliser le logiciel AirCheck™ Manager pour transférer les résultats vers un PC et créer des rapports de qualité professionnelle. AirCheck Manager permet de comparer les informations des différentes sessions de tests pour faire apparaître les changements du réseau LAN sans fil.

Enregistrement de votre produit

L'enregistrement du produit auprès de Fluke Networks vous permet d'accéder à des informations importantes, aux mises à jour des produits, à des procédures de dépannage et à d'autres services d'assistance. Pour enregistrer le produit, remplissez le formulaire sur le site Web de Fluke Networks www.flukenetworks.com/MyAccountFR.

La base de connaissances de Fluke Networks

La base de connaissances de Fluke Networks apporte des réponses à des questions fréquemment posées sur les produits Fluke Networks et regroupe des informations sur la technologie et les procédures de test des câblages et réseaux. Pour consulter la base de connaissances, accédez au site www.flukenetworks.com/fr, puis cliquez sur **Support** > **Base de connaissances**.

Pour contacter Fluke Networks



www.flukenetworks.com/fr



support@flukenetworks.com



+1-425-446-4519

- Australie : 61 (2) 8850-3333 ou 61 (3) 9329 0244
- Pékin : 86 (10) 6512-3435
- Brésil : 11 3759 7600
- Canada : 1-800-363-5853
- Europe : +31-(0) 40 2675 600
- Hong Kong : 852 2721-3228
- Japon : 03-6714-3117
- Corée : 82 2 539-6311
- Singapour : +65-6799-5566
- Taïwan : (886) 2-227-83199
- Etats-Unis : 1-800-283-5853

Pour obtenir des numéros de téléphone supplémentaires, consultez notre site Web.

Informations sur la sécurité

Le tableau 1 décrit les symboles de sécurité utilisés sur le testeur et dans ce manuel.

Tableau 1. Symboles de sécurité

	Avertissement ou Attention : risque d'endommagement ou de destruction de l'équipement ou du logiciel. Reportez-vous aux explications fournies dans ce manuel.
	Avertissement : risque d'électrocution.
	Ne jetez pas de produits contenant des cartes de circuit dans les bennes à ordures. Consultez la législation locale pour connaître les procédures de mise au rebut.
	Cet équipement contient une radio de classe 2.

Avertissement

N'utiliser que l'adaptateur secteur fourni pour recharger la batterie.

Attention

En cas d'utilisation d'une antenne externe, n'utiliser que l'antenne créée par Fluke Networks pour le testeur AirCheck. Le testeur ne fonctionne pas correctement avec d'autres antennes.

Déballage

Le testeur Wi-Fi AirCheck est livré avec les accessoires mentionnés dans la liste ci-dessous. Si un article est endommagé ou absent, notifiez le distributeur qui vous a vendu le produit.

Testeur Wi-Fi AirCheck

- AirCheck avec bloc-batterie rechargeable
- Adaptateur secteur
- Câble USB
- Mallette de transport

- Guide d'introduction
- CD des manuels de produits
- CD d'installation AirCheck Manager

Kit de dépannage de première ligne AirCheck

- AirCheck avec bloc-batterie rechargeable
- Batterie rechargeable supplémentaire
- LinkRunner™ Pro
- Antenne directionnelle externe munie d'un connecteur RSMA
- Détecteur PoE
- Adaptateur secteur
- Câble USB
- Mallette de transport
- Guide d'introduction
- CD des manuels de produits
- CD d'installation AirCheck Manager

Caractéristiques physiques

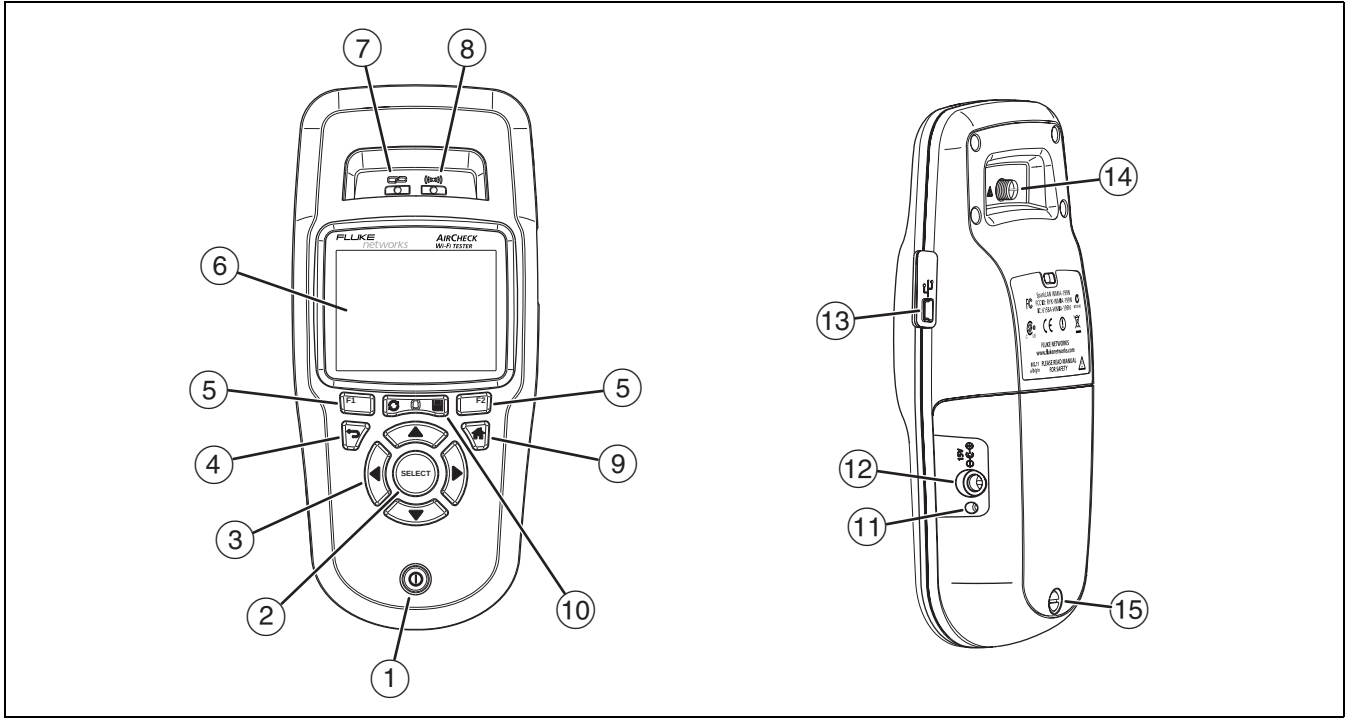


Figure 1. Caractéristiques physiques

ffy01.eps

- ① Interrupteur marche/arrêt.
- ② Permet de sélectionner un élément sur l'écran.
- ③ Touches de navigation.
- ④ Affiche l'écran précédent.
- ⑤ Touches programmables. La fonction de la touche programmable est indiquée au-dessus de la touche.
- ⑥ Ecran LCD couleur.
- ⑦ Le témoin clignote lorsque le testeur essaie de se connecter à un réseau LAN sans fil. Le témoin s'allume lorsque le testeur est connecté à un réseau LAN sans fil.
- ⑧ Le témoin clignote lorsque le testeur transmet les données.
- ⑨ Affiche l'écran d'accueil.
- ⑩  : Efface toutes les données collectées pendant la séquence des tests actuelle. Les résultats enregistrés en mémoire ne sont pas effacés.  : Enregistre toutes les données dans un fichier de session. Voir page 62.
- ⑪ Le témoin s'allume lorsque l'adaptateur secteur est branché. Le témoin est rouge lorsque la batterie se charge ; il est vert lorsque la batterie est à pleine charge.
- ⑫ Connecteur de l'adaptateur secteur.
- ⑬ Port USB pour la connexion à un PC.
- ⑭ Connecteur de l'antenne directionnelle externe. Voir page 58.
- ⑮ Vis du bloc-batterie.

Charge et durée de vie de la batterie

Chargez la batterie pendant environ 4 heures avant de l'utiliser pour la première fois.

Pour charger la batterie, branchez l'adaptateur secteur au connecteur de la batterie (12 dans la figure 1). Vous pouvez utiliser le testeur pendant que la batterie se recharge.

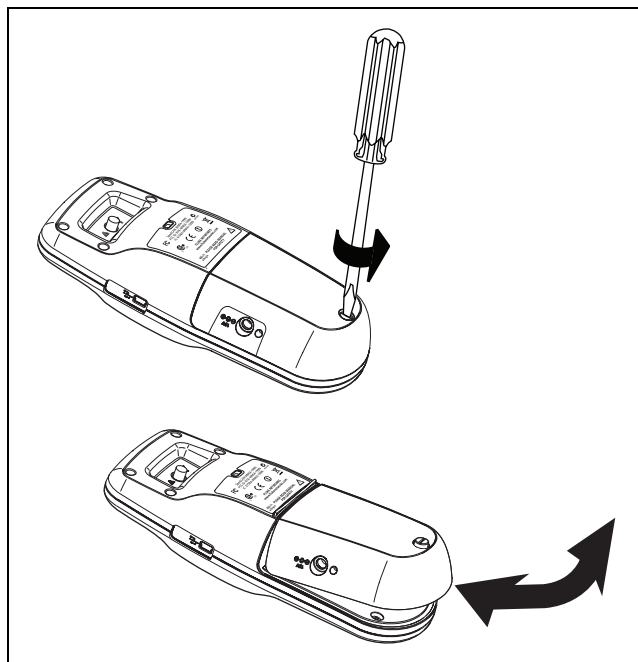
La figure 2 montre comment remplacer la pile.

Lorsque le testeur est inactif, la batterie se charge en 3 heures environ.

Remarque

La batterie ne se charge pas si la température interne du testeur est supérieure à 45 °C (113 °F).

La durée de vie de la batterie est d'environ 5,5 h en fonctionnement normal. L'icône qui s'affiche dans le coin supérieur gauche indique l'état de la batterie. Voir Figure 3 page 13.



ffy14.eps

Figure 2. Comment retirer la batterie

Configuration minimum pour des performances optimales

Pour obtenir les meilleures performances, configurez un profil à l'aide du logiciel AirCheck Manager, puis chargez-le sur le testeur. Les données contenues dans le profil permettent au testeur d'exécuter les tâches suivantes :

- Connexion aux réseaux exigeant des identifiants de sécurité.
- Affichage de l'état d'autorisation correct pour chaque point d'accès. Vous pouvez ainsi visualiser rapidement les points d'accès autorisés sur le réseau.
- Envoi de commandes ping aux principaux périphériques réseau.

Voir « Configuration du testeur » à la page 14.

Informations fournies sur un réseau

Les sections ci-dessous présentent les informations que le testeur fournit sur un réseau.

Composition du réseau LAN sans fil

Quels sont les réseaux LAN sans fil disponibles ?	Sélectionnez Réseaux pour afficher la liste des réseaux LAN sans fil et des points d'accès connectés à chaque réseau. Pour afficher tous les points d'accès disponibles dans la zone, sélectionnez Points d'accès . Voir page 24.
Quels sont les points d'accès disponibles ? L'intensité du signal est-elle suffisante ?	Sélectionnez Points d'accès pour afficher la liste des points d'accès disponibles dans la zone avec l'intensité du signal de chaque point d'accès. Voir page 28.
Le point d'accès est-il correctement configuré ?	Sélectionnez Points d'accès , mettez un point d'accès en surbrillance, puis appuyez sur  . Voir page 28.
Y a-t-il de nouveaux points d'accès dans la zone ? Certains sont-ils inaudibles ?	Sauvegardez la session de tests, puis utilisez AirCheck Manager pour comparer la liste de points d'accès à une autre liste enregistrée dans le logiciel. Voir pages 54 et 65.
Quels clients sans fil utilisent le réseau ?	Sélectionnez Outils , puis Répertorier les clients . Voir page 49.

Connectivité des périphériques au réseau

Le testeur permet de vérifier la connectivité.

Remarque

*Vous ne pouvez vous connecter aux réseaux sécurisés que si un profil avec identifiants de sécurité est configuré sur le testeur. Si les identifiants de sécurité ne sont pas disponibles, la touche programmable affiche  **Connexion***. Voir page 14.*

Les périphériques peuvent-il se connecter à ce réseau (SSID) en tant que clients ?	Sélectionnez Réseaux , sélectionnez un réseau, puis appuyez sur  Connexion . Voir page 42.
Les périphériques peuvent-il se connecter à ce point d'accès (BSSID) ?	Sélectionnez Points d'accès , sélectionnez un point d'accès, puis appuyez sur  Connexion . Voir page 42.
En cas d'échec de la connexion d'un périphérique à un réseau ou à un point d'accès, à quel stade la connexion échoue-t-elle ?	Consultez le journal de connexion. Voir page 45.
Les périphériques peuvent-ils adresser des commandes ping à ce périphérique réseau ?	Faites un test ping. Voir page 46.
La carte réseau de ce client fonctionne-t-elle correctement ?	Sélectionnez Outils , puis Répertoire des clients pour vérifier si le client transmet les trames de demande de vérification et afficher des paramètres de base, tels que le canal et les identifiants SSID utilisés par le client au cours des vérifications. Voir page 50.

Causes des ralentissements de performances réseau et des pertes de connexion

L'intensité du signal est-elle suffisante ?	Sélectionnez Points d'accès . L'écran Points d'accès indique l'intensité du signal pour chaque point d'accès. Sélectionnez un point d'accès pour afficher plus de détails sur l'intensité du signal et l'encombrement. Voir page 32.
Le réseau est-il surchargé ?	Sélectionnez Canaux pour afficher une vue générale de l'utilisation des canaux et le nombre de points d'accès qui utilisent chaque canal. Pour afficher un graphique, sélectionnez un canal, puis appuyez sur  . Voir page 38.
Les clients qui utilisent un canal ou un point d'accès sont-ils trop nombreux ?	Sélectionnez Outils , puis Répertorier les clients pour afficher le nombre de clients qui utilisent un canal ou un point d'accès. Voir page 49.
Les clients qui utilisent un débit de transmission peu élevé sont-ils trop nombreux ?	Sélectionnez Outils , puis Répertorier les clients pour afficher les débits de transmission des clients. Voir page 49.
Y a-t-il des interférences non 802.11 sur ce canal ?	Sélectionnez Canaux . Les interférences non 802.11 sont indiquées en gris. Ce bruit peut interférer avec les connexions ou les performances du réseau sans fil. Le bruit non 802.11 peut provenir de différentes sources : fours à micro-ondes, téléphones sans fil, appareils Bluetooth®, détecteurs de mouvement, caméras sans fil et autres appareils sans fil. Voir page 40.

Sécurité du réseau

Les réseaux offrent-ils le niveau de sécurité attendu ?	Sélectionnez Réseaux. Les réseaux qui comportent des points d'accès non sécurisés sont signalés par un cadenas ouvert rouge (). Voir page 24.
Y a-t-il des réseaux ad-hoc dans la zone ?	Sélectionnez Réseaux. Les réseaux qui comportent des clients ad hoc sont signalés par l'icône () dans la colonne SSID. Les clients ad hoc peuvent présenter des risques pour la sécurité du réseau ou violer les règles d'utilisation du réseau. Voir page 24.
Y a-t-il des points d'accès indésirables dans la zone ? Lesquels ?	Les points d'accès ont l'état Périphérique non autorisé  jusqu'à ce que vous les changiez d'état. Si vous définissez l'état de tous les points d'accès du réseau, les nouveaux points d'accès potentiellement indésirables seront signalés par l'état . Si vous savez qu'un point d'accès est indésirable, vous pouvez lui donner l'état «  Périphérique signalé ». Voir page 22. Pour donner un état d'autorisation, sélectionnez Points d'accès, sélectionnez un point d'accès, puis appuyez sur  ACL. Pour localiser un point d'accès, sélectionnez-le, puis appuyez sur  Localiser dans l'écran Détails du point d'accès. Voir page 54.

Localisation d'un point d'accès

Sélectionnez **Points d'accès**, sélectionnez un point d'accès, puis appuyez sur  **Localiser** dans l'écran **Détails du point d'accès**. Voir page 54. L'antenne directionnelle externe Fluke Networks disponible en option permet de retrouver plus rapidement les points d'accès. Voir page 54.

Réseaux ou points d'accès disponibles lorsque je me déplace

Triez la liste par ordre décroissant dans la colonne d'horodatage (). Appuyez sur , puis déplacez-vous. Les nouveaux réseaux ou points d'accès disponibles apparaissent en début de liste. Voir page 25 ou 29.

Consignation de l'état du réseau et de la session de test

Enregistrez la session (voir page 54), puis utilisez le logiciel AirCheck Manager pour transférer les données sur un PC et créer un rapport. Voir page 65.

L'écran d'accueil

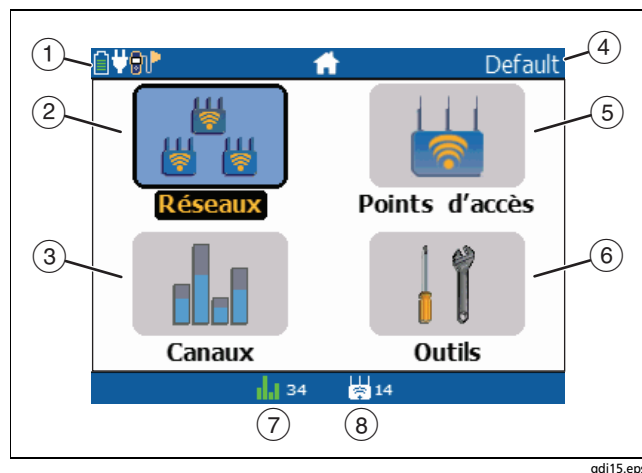


Figure 3. L'écran d'accueil

- 1  Indique l'état de la batterie. L'icône clignote lorsque la charge de la batterie est faible. Branchez l'adaptateur secteur pour charger la batterie et vous assurer que le testeur continue de fonctionner.

-  Indique que l'antenne externe est branchée.
- ② **Réseaux** : Recherche les réseaux LAN sans fil. Voir page 23.
- ③ **Canaux** : Affiche le taux d'utilisation des canaux WLAN. Voir page 38.
- ④ Le nom du profil que le testeur utilise. Le profil est **Default** (Par défaut) si vous n'avez pas chargé de profil différent. Le nom du profil est suivi d'un astérisque si vous avez modifié un paramètre sur le testeur depuis le chargement ou l'enregistrement du profil. Voir page 64.
- ⑤ **Points d'accès** : Recherche les points d'accès. Voir page 23.
- ⑥ **Outils** : Permet de gérer les fichiers et les paramètres. Permet également d'afficher la liste des clients qui transmettent les sondages (voir page 49).
- ⑦ Le canal actuellement surveillé par le testeur. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20.
- ⑧ Nombre de points d'accès détectés par le testeur. Si l'option **Regrouper points d'accès virtuels** est activée, ce nombre ne comprend pas les points d'accès virtuels. Voir page 17.

Configuration du testeur

Pour modifier les paramètres sur le testeur, sélectionnez

Outils sur l'écran d'accueil. Voir le tableau 2 page 17.

Changer les paramètres linguistiques et nationaux

- 1 Sélectionnez **Tools (Outils)**.
- 2 Pour modifier la langue des écrans, sélectionnez **Set Language (Définir la langue)**. Mettez la langue choisie en surbrillance, puis appuyez sur  **Save (Enregistrer)**.
- 3 Pour modifier le pays, sélectionnez **Définir le pays**, puis le pays où le testeur est utilisé. Voir page 19.

Créer un profil pour se connecter à des réseaux sécurisés

Les profils sont des fichiers contenant les paramètres pour les réseaux et le testeur. Les paramètres de réseau comprennent les identifiants de sécurité. Ces identifiants permettent au testeur de se connecter aux réseaux et d'effectuer les tests d'émission d'écho (tests ping). Les profils peuvent avoir des mots de passe pour interdire aux utilisateurs non autorisés d'accéder aux identifiants de sécurité du réseau dans AirCheck Manager et d'utiliser le testeur pour se connecter à des réseaux sécurisés.

Vous pouvez enregistrer les paramètres du testeur dans un profil ou utiliser AirCheck Manager pour créer le profil sur un PC.

L'écran d'accueil affiche le nom du profil utilisé par le testeur. Le nom du profil est suivi d'un astérisque si vous avez modifié un paramètre sur le testeur depuis le chargement ou l'enregistrement du profil. Le testeur enregistre les modifications dans un fichier temporaire, qui est une copie du profil affiché sur l'écran d'accueil. Le testeur utilise le fichier temporaire en tant que profil actuel. Lorsque vous enregistrez le profil, le testeur copie les modifications dans le profil qui s'affiche sur l'écran d'accueil.

Les profils créés dans AirCheck Manager contiennent les paramètres suivants :

- un mot de passe pour le profil
- les identifiants de sécurité des réseaux

Remarque

Pour créer un profil intégrant les identifiants de sécurité d'un réseau ou le mot de passe d'un profil, vous devez utiliser AirCheck Manager.

- les adresses IP et l'état d'autorisation des réseaux (SSID) et des points d'accès
- les adresses IP pour les tests d'émission d'écho

- tous les paramètres 802.11 (par exemple, **Activer la bande 2,4 GHz** et **Activer la bande 5 GHz**. Voir page 17).
- le pays
- le réglage du seuil pour l'affichage incrémental

Si vous enregistrez le profil pendant que vous l'utilisez sur le testeur, ce dernier ajoute les paramètres au profil :

- le réglage sonore de la fonction de localisation
- le paramètre d'arrêt automatique
- les séquences d'ordre de tri pour les listes de réseaux, des points d'accès et des clients

Pour transférer le profil d'un PC vers le testeur

- 1 Utilisez le **Gestionnaire de profils** dans AirCheck Manager pour créer un profil.
- 2 Utilisez le câble USB fourni avec le testeur pour relier le testeur au PC.
- 3 Utilisez la fonction de transfert du **Gestionnaire de profils** pour transférer le profil vers le testeur.

Pour charger un profil présent dans le testeur

- 1 Sélectionnez **Outils > Gérer les fichiers**, puis **Charger le profil**.

- 2 Mettez un profil en surbrillance, appuyez sur  puis sur  **Charger**.

Remarque

*Si le fichier n'est pas un profil valide ou si l'extension n'est pas « .ACP », le testeur affiche le message « **Ne peut charger le profil sélectionné** ».*

- 3 Entrez le mot de passe du profil s'il y a lieu.

Remarque

*Le mot de passe ne doit être entré que lorsque le profil est chargé sur le testeur pour la première fois. Pour protéger de nouveau tous les profils par mot de passe, sélectionnez **Outils > Restaurer aux réglages d'usine**.*

Pour enregistrer les paramètres actuels en tant que profil

- 1 Sélectionnez **Outils > Gérer les fichiers**, puis **Enregistrer le profil**.
 - Pour enregistrer le profil sous le nom de fichier affiché, appuyez sur  **Enregistrer**. Le testeur enregistre le profil dans le dossier « PROFILES » (PROFILS).

-suite-

- Pour remplacer un profil enregistré sur le testeur, mettez le profil en surbrillance, appuyez sur , sur  **Enregistrer**, puis sur  **OK**.
- Pour modifier le nom du fichier, appuyez sur  **Modifier**.

Remarque

Les noms de fichier sont limités à 8 caractères avec une extension de 3 caractères maximum.
L'extension doit être « .ACP » pour afficher le profil dans AirCheck Manager.

- Pour supprimer des caractères du nom du fichier, appuyez sur  **Supprimer**.
- Pour ajouter des caractères au nom de fichier, utilisez   pour mettre en surbrillance un caractère, puis appuyez sur .
- Pour déplacer le curseur dans le nom de fichier, mettez le nom de fichier en surbrillance, puis appuyez sur  .
- Pour enregistrer le profil en utilisant le nom de fichier modifié, appuyez sur  **Terminé**, puis sur  **Enregistrer**. Le testeur enregistre le profil dans le dossier « PROFILES » (PROFILS).

Paramètres

Le tableau 2 affiche les paramètres que vous pouvez créer sur le menu **Outils**.

Lorsque vous modifiez un paramètre, appuyez sur  **Enregistrer** pour enregistrer les modifications. Pour quitter l'application sans enregistrer vos paramètres, appuyez sur  **Annuler**.

Remarque

Pour enregistrer vos paramètres dans un profil, sélectionnez **Outils > Enregistrer le profil**.

Tableau 2. Paramètres sur le menu Outils

Gérer les paramètres 802.11 <i>Remarque</i> <i>Ces paramètres affectent le mode d'identification et d'affichage des points d'accès. Veillez à bien les maîtriser avant d'utiliser le testeur.</i>	Permet de définir les options des listes de points d'accès et des canaux. • Activer la bande 2,4 GHz, Activer la bande 5 GHz : Sélectionnez l'une ou les deux bandes de fréquence pour afficher les réseaux et les points d'accès de l'une ou des deux bandes. • Transmettre des sondages : Pour détecter des points d'accès, le testeur écoute les diffusions SSID sur chaque canal. L'appareil ne peut détecter que les points d'accès qui diffusent leur identifiant SSID alors que le testeur occupe le même canal. Pour accélérer la recherche, le testeur transmet des trames de demande de sondage par défaut pour obtenir les réponses des points d'accès. Etant donné que les sondages accroissent le taux d'utilisation des canaux, le testeur ne transmet pas les sondages lorsque l'utilisateur examine les écrans d'utilisation des canaux ou branche l'antenne externe.
---	--

-suite-

Tableau 2. Paramètres sur le menu Outils (suite)

Gérer les paramètres 802.11 (suite) <i>Remarque</i> <i>Ces paramètres affectent le mode d'identification et d'affichage des points d'accès. Veillez à bien les maîtriser avant d'utiliser le testeur.</i>	Regrouper points d'accès virtuels : Lorsqu'un point d'accès diffuse plusieurs adresses MAC (BSSID), les adresses MAC sont des points d'accès virtuels. Les points d'accès virtuels peuvent prendre en charge différents réseaux à partir d'un point d'accès physique. Un point d'accès utilisant deux radios pour diffuser plusieurs adresses MAC peut prendre en charge des réseaux sur différents canaux. Lorsque l'option Regrouper points d'accès virtuels est activée, les points d'accès virtuels sont affichés en tant que point d'accès unique dans la liste Points d'accès. Si le point d'accès diffuse un nom (affiché dans la colonne Name/MAC (Nom/MAC), le nombre d'identifiants SSID qu'il prend en charge s'affiche dans la colonne SSID. Par exemple, « 2 SSID » s'affiche dans la colonne. Si le point d'accès ne diffuse pas de nom, il remplace le dernier chiffre de l'adresse MAC par un astérisque dans la colonne Name/MAC (Nom/MAC). Pour afficher les adresses MAC et les identifiants SSID associés aux points d'accès virtuels, sélectionnez le point d'accès dans la liste Points d'accès. Par défaut, ce paramètre est activé. Griser points d'accès inaudibles : Si le testeur n'a pas entendu de point d'accès pendant quatre cycles sur tous les canaux, le point d'accès apparaît grisé dans la liste Points d'accès. Ce réglage est recommandé par défaut. Supprimer points d'accès inaudibles : Si le testeur n'a pas entendu de point d'accès pendant quatre cycles sur tous les canaux, il supprime ce point d'accès de la liste Points d'accès.
---	---

Tableau 2. Paramètres sur le menu Outils (suite)

Utiliser réglage de signal pers.	Permet de régler les mesures d'intensité du signal en fonction des autres périphériques. Voir page 61.
Définir la date et l'heure	Permet d'afficher l'heure et la date que le testeur incorpore aux résultats enregistrés. Utilisez  pour sélectionner un paramètre et  pour le modifier.
Définir les seuils	Permet de définir les seuils des couleurs dans les affichages incrémentaux des mesures. Voir page 21.
Définir le pays	Les canaux interdits dans le pays sélectionné sont rouges sur les écrans Utilisation du canal , Détails util. canal et Détails du point d'accès . Voir « Fonctionnement 802.11d » à la page 20. Les points d'accès qui transmettent un code de pays non compatible avec ce réglage sont signalés par des barres rouges dans la colonne 802.11 .
Définir la langue	Définit la langue de l'interface utilisateur.
Gérer l'alimentation	Lorsque cette option est activée, le testeur s'éteint automatiquement si aucune touche n'est activée pendant 10 minutes. Le testeur n'enregistre pas de session de tests lorsqu'il s'éteint automatiquement. Il n'enregistre pas les changements apportés au profil. Le testeur ne s'éteint pas automatiquement si l'adaptateur secteur est branché. Appuyez sur  Enregistrer pour enregistrer vos paramètres. Pour quitter l'application sans enregistrer vos paramètres, appuyez sur  Annuler .
Restaurer aux réglages d'usine	Rétablit toutes les valeurs de réglage par défaut. Voir l'annexe B.

Fonctionnement 802.11d

Si un point d'accès utilise la norme 802.11d, il transmet un code de pays ISO et ses balises et réponses de sondage. Lorsque le testeur reçoit ce code, il ne transmet que sur les canaux autorisés dans le pays en question et n'utilise que les niveaux de puissance autorisés.

Si le testeur ne reçoit pas de code de pays, le testeur fonctionne en « mode mondial » :

- Le testeur n'utilise que les canaux et les niveaux de puissance qui sont autorisés dans tous les pays. Les canaux vont de 1 à 11 dans la bande 2,4 GHz.
- Le testeur ne transmet pas les sondages sur les canaux 12, 13 et 14 de la bande 2,4 GHz.
- Le testeur ne transmet pas dans la bande 5 GHz, sauf s'il détecte que des points d'accès fonctionnent dans cette bande.
- Le testeur utilise la puissance de transmission la plus faible qui est autorisée dans tous les pays.

Les barres en bas de l'affichage et les icônes sur les écrans de réseaux et des points d'accès affichent l'état du code de pays :

 Barres vertes : Le testeur a reçu un code de pays d'un ou de plusieurs points d'accès. Tous les codes de pays reçus sont les mêmes. Ils sont tous compatibles avec le paramètre **Outils > Définir le pays**. Le testeur fonctionne sur les canaux et utilise les niveaux de puissance qui sont autorisés dans ce pays.

 Barres blanches : Le testeur n'a pas reçu de code de pays. Le testeur fonctionne en mode mondial.

 Barres rouges : Le testeur a reçu un code de pays différent du paramètre défini dans **Outils > Définir le pays**. Pour identifier le réseau ou le point d'accès émetteur du code, sélectionnez **Réseaux** ou **Points d'accès**, puis recherchez les barres rouges dans la colonne **802.11**.

L'écran **Détails du point d'accès** affiche le code de pays 802.11d transmis par le point d'accès. L'annexe C indique les pays associés aux codes.

Modifier les seuils des couleurs dans les affichages incrémentaux

Les couleurs des affichages incrémentaux indiquent que l'intensité du signal, le bruit et le rapport signal/bruit sont au-dessus ou en dessous des seuils spécifiés. Vous pouvez modifier ces seuils de façon à ce que les couleurs indiquent si le signal est conforme aux exigences du réseau.

Pour modifier les seuils associés aux couleurs

- 1 Sélectionnez **Outils**.
- 2 Sélectionnez **Définir les seuils**.
- 3 Sélectionnez un élément. La figure 4 indique comment modifier les seuils des couleurs.

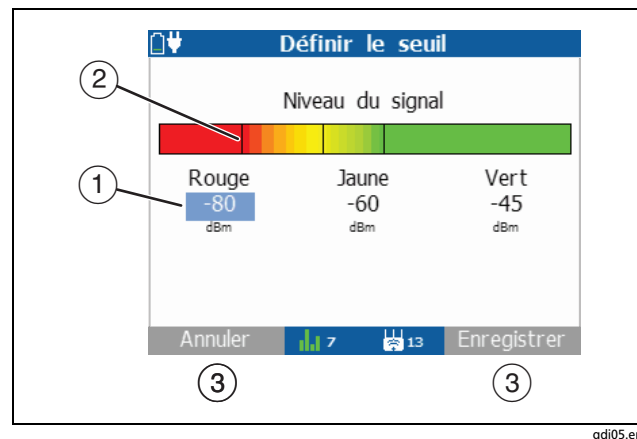


Figure 4. Modifier les seuils des couleurs dans un affichage incrémental

- ① Utilisez pour sélectionner une couleur. Utilisez pour augmenter ou diminuer la valeur mesurée liée à la couleur.
- ② Les traits indiquent l'emplacement de la valeur sur l'affichage incrémental.
- ③ Appuyez sur **Enregistrer** pour enregistrer vos paramètres. Pour quitter l'application sans enregistrer vos paramètres, appuyez sur **Annuler**.

Donner un état d'autorisation aux points d'accès

Lorsque vous définissez l'état d'autorisation de chaque point d'accès, vous pouvez rapidement indiquer si celui-ci fait partie intégrante du réseau. Les points d'accès sont signalés par un triangle jaune (⚠) dans la colonne de la liste de contrôle d'accès (ACL) tant que l'utilisateur ne modifie pas l'état.

Pour donner un état d'autorisation à un point d'accès

- 1 Sélectionnez **Points d'accès**.
- 2 Si un point d'accès est doté de plusieurs adresses MAC et si vous souhaitez donner des états d'autorisation différents à ces adresses MAC, sélectionnez le point d'accès.
- 3 Sélectionnez un point d'accès, puis appuyez sur  **ACL**.
- 4 Mettez en surbrillance un état sur l'écran **Etat d'autorisation**, appuyez sur , puis sur .

 **Périphérique non autorisé** : Le point d'accès ne possède pas d'état d'autorisation.

 **Périphérique autorisé** : Le point d'accès est autorisé à se connecter au réseau.

 **Périphérique voisin** : Le point d'accès n'est pas autorisé à se connecter au réseau mais ne constitue pas de menace à la sécurité du réseau.

 **Périphérique invité** : Le point d'accès est autorisé à se connecter au réseau mais en disposant d'un accès limité.

 **Périphérique signalé** : Vous pouvez utiliser ce symbole pour les points d'accès à surveiller. Par exemple, si vous pensez qu'un point d'accès est indésirable, vous pouvez placer un drapeau en regard de celui-ci en attendant de détenir tous les détails à son sujet.

Lorsque l'utilisateur éteint son testeur, les paramètres ACL sont enregistrés dans le profil temporaire.

Remarque

Si un point d'accès ne transmet pas, AirCheck Manager vous permet d'accorder un état d'autorisation au point d'accès dont l'adresse MAC est connue. Enregistrez l'état dans un profil avant de le transférer vers le testeur.

Détection des réseaux et des points d'accès

Remarque

*Par défaut, le testeur recherche les signaux d'accès sans fil sur les bandes de fréquence 2,4 GHz (b/g/n) et 5 GHz (a/n) pour identifier les points d'accès sans fil. Pour modifier ce paramètre, sélectionnez **Outils**, puis **Gérer les paramètres 802.11**.*

Pour détecter les réseaux et les points d'accès

- 1 Sur l'écran d'accueil, sélectionnez **Réseaux** ou **Points d'accès**. Le testeur affiche la liste **Réseaux** ou **Points d'accès** (figures 5 et 6).
- 2 Pour afficher les détails d'un point d'accès (figure 7), appuyez sur   pour sélectionner le point d'accès, puis appuyez sur .

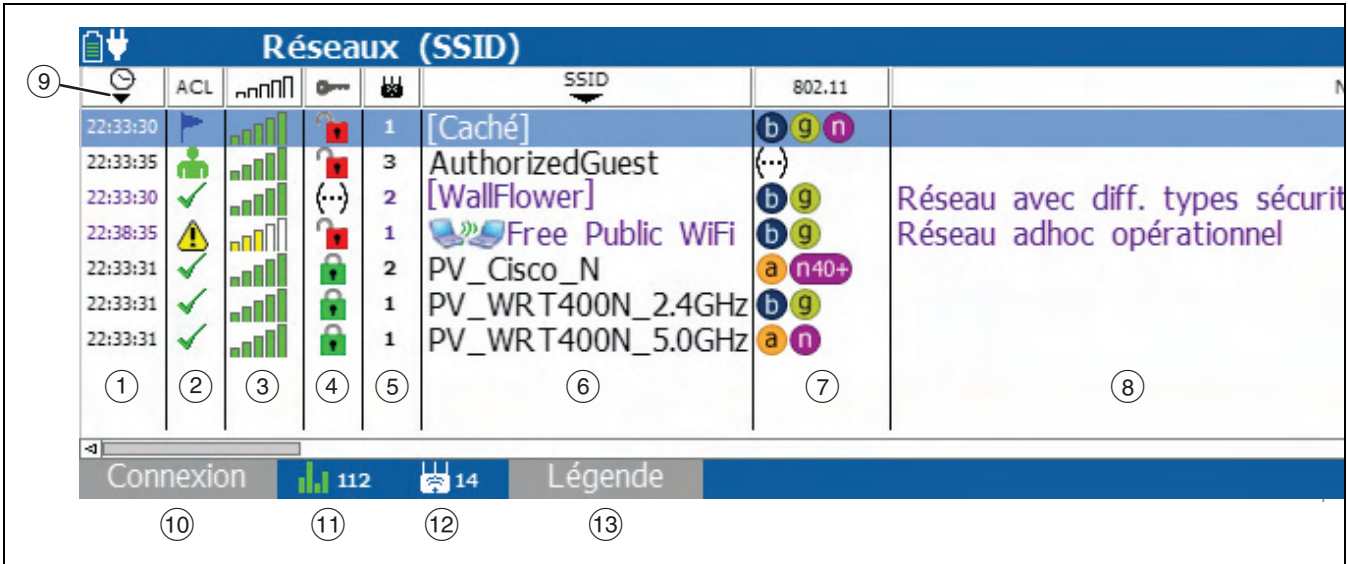


Figure 5. Liste des réseaux (SSID)

gdj03.eps

- ①  : L'heure à laquelle le testeur a entendu le réseau pour la première fois. Pour voir les réseaux qui deviennent disponibles à mesure que vous vous déplacez, triez la liste par ordre décroissant d'après la colonne d'horodatage.
Appuyez sur , puis déplacez-vous. Les nouveaux réseaux disponibles apparaissent en haut de la liste. Si l'option **Griser points d'accès inaudibles** est activée, les réseaux hors de portée sont grisés.
- ② **ACL** : L'état d'autorisation du point d'accès. L'état par défaut est **Périphérique non autorisé** . Changez l'état de chaque point d'accès pour révéler sa relation à votre réseau. Voir page 22.
(...) : Les points d'accès sur le réseau n'ont pas tous le même état d'autorisation.
- ③  : Intensité maximum du signal de tous les points d'accès pour un identifiant **SSID** réseau donné. Vous pouvez modifier les seuils des couleurs dans les affichages incrémentaux. Voir page 21.
- ④  : L'état de sécurité du réseau :
 Cadenas ouvert rouge : La sécurité n'est pas activée pour le réseau.

 Cadenas refermé jaune : Un ou plusieurs points d'accès utilisent le protocole de sécurité WEP ou Cisco LEAP. Ces protocoles sont moins fiables que d'autres options.

 Cadenas refermé vert : Tous les points d'accès utilisent des protocoles de sécurité qui sont plus sécurisés que WEP ; par exemple, WPA ou WPA2.

(...) : Tous les points d'accès du réseau n'utilisent pas le même type de sécurité. Par exemple, certains utilisent WEP, d'autres WPA.

- ⑤  : Nombre de points d'accès que le testeur entend dans la zone ciblée.
- ⑥ **SSID** : Identificateur SSID (Service Set Identifier). Nom du réseau sans fil.
Les réseaux que le testeur n'a pas entendus récemment apparaissent en grisé si l'option **Griser points d'accès inaudibles** est activée (voir page 18).
 : Le réseau utilise des périphériques ad hoc. Ces périphériques communiquent directement avec d'autres périphériques, et non pas en empruntant un point d'accès faisant partie du réseau. Les périphériques ad-hoc peuvent donner aux pirates un accès aux données échangées sur le réseau. (Certaines directives informatiques autorisent néanmoins les périphériques ad-hoc.)

[Caché] : Le réseau ne diffuse pas son identifiant SSID.

Si un SSID s'affiche entre crochets, le testeur a détecté le SSID caché dans les paquets d'autres clients sans fil. Dans AirCheck Manager, ces SSID s'affichent sans crochets.

- ⑦ **802.11** : Les normes 802.11 que les points d'accès utilisent dans le réseau :
-  **802.11a** : Utilise la bande 5 GHz.
 -  **802.11b** : Utilise la bande 2,4 GHz.
 -  **802.11g** : Utilise la bande 2,4 GHz.
 -  **802.11n** : Peut être utilisé dans les bandes 2,4 GHz ou 5 GHz.
-  **Barres rouges** : Le testeur a reçu un code de pays 802.11d du point d'accès. Le pays est différent du pays sélectionné dans l'option **Outils > Définir le pays** dans le testeur.
-  : Un ou plusieurs points d'accès utilisent un canal couplé. Les points d'accès qui utilisent la norme 802.11n peuvent coupler un canal à un canal d'extension au-dessus () ou en dessous () pour former un canal 40 MHz. Ce canal plus large permet d'obtenir un meilleur débit réseau.

(...) : Les points d'accès du réseau n'utilisent pas tous la même norme 802.11.

- ⑧ **Notes (Remarques)** : Appuyez sur  pour atteindre le champ de notes. Le testeur ajoute des notes automatiquement. Voir page 35. Les réseaux associés à des notes sont indiqués en violet.

(...) : Le réseau est accompagné de plusieurs remarques. Pour afficher toutes les notes, sélectionnez le réseau, puis appuyez sur  deux fois pour afficher l'écran **Détails du point d'accès**.

- ⑨  : **Tri 1**, ordres de tri croissant et décroissant
 : **Tri 2**, ordres de tri croissant et décroissant

Pour trier la liste par ordre croissant ou décroissant, appuyez sur  et sur  pour sélectionner un en-tête de colonne, puis appuyez sur  ou  **Tri 1**. Par exemple, pour retrouver facilement le point d'accès avec le signal le plus fort, sélectionnez  en haut de la colonne, puis appuyez sur  ou  **Tri 1**. Le point d'accès avec le signal le plus fort est placé en haut de la liste.

Pour appliquer un ordre de tri secondaire, sélectionnez un autre en-tête de colonne, puis appuyez sur  **Tri 2**.

- ⑩ Appuyez sur  **Connexion** pour vous connecter au réseau sélectionné. Voir page 42.

Si le testeur ne peut se connecter au réseau sélectionné, le bouton indique « **Connexion*** ». Voir page 42.

- ⑪  : Le canal actuellement surveillé par le testeur. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20.
- ⑫  : Nombre de points d'accès que le testeur entend dans la zone ciblée. Si l'option **Regrouper points d'accès virtuels** est activée, ce nombre ne comprend pas les points d'accès virtuels. Voir page 17.
- ⑬ Pour afficher la description des icônes de l'écran **Réseaux**, appuyez sur  **Légende**.

Pour afficher les détails des points d'accès d'un réseau, appuyez sur   pour sélectionner un réseau, puis appuyez sur . Voir figure 6.

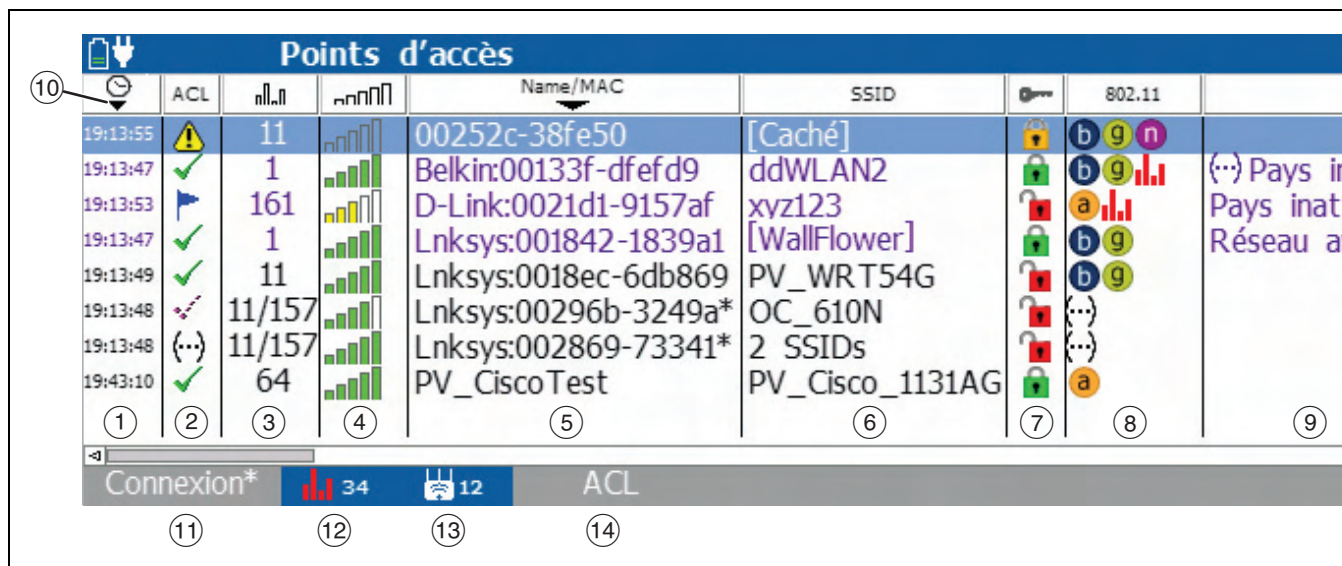


Figure 6. Liste des points d'accès

gdj02.eps

- ①  : L'heure à laquelle le testeur a entendu le point d'accès pour la première fois. Pour afficher les nouveaux points d'accès disponibles quand vous vous déplacez dans une zone, triez la liste par ordre décroissant dans la colonne d'horodatage.
- Appuyez sur , puis déplacez-vous. Les nouveaux points d'accès disponibles sont ajoutés en début de liste. Si l'option **Griser points d'accès inaudibles** est activée, les réseaux hors de portée sont grisés.
- ② **ACL** : L'état d'autorisation du point d'accès. L'état par défaut est **Périphérique non autorisé** . Changez l'état de chaque point d'accès pour révéler sa relation à votre réseau. Voir page 22.
- (...) : Les points d'accès virtuels ou les adresses MAC d'un même point d'accès présentent des paramètres d'état d'autorisation différents. On leur donne habituellement le même état d'autorisation.
- ③  : Le canal que le point d'accès utilise.
- ④  : L'intensité du signal. Si plusieurs points d'accès sont disponibles, cette colonne indique la puissance du signal le plus fort. Vous pouvez modifier les seuils des couleurs dans les affichages incrémentaux. Voir page 21.
- ⑤ **Name/MAC** (Nom/MAC) : Le nom ou l'adresse MAC du point d'accès. L'adresse commence par le préfixe de l'abréviation du fournisseur, si ce préfixe est disponible. Se reporter à la section « oui_abbr.txt » page 64.
- * : Le point d'accès diffuse plusieurs adresses MAC (BSSID). Pour afficher les adresses MAC, sélectionnez le point d'accès. Se reporter à la section « **Regrouper points d'accès virtuels** » page 18.
- Les points d'accès que le testeur n'a pas entendus récemment apparaissent en grisé si l'option **Griser points d'accès inaudibles** est activée (voir page 18).
- ⑥ **SSID** : Identificateur SSID (Service Set Identifier). Le nom du réseau.
- Si le point d'accès prend en charge plusieurs SSID, sélectionnez le point d'accès pour les afficher. Se reporter à la section « **Regrouper points d'accès virtuels** » page 18.
- Si vous ouvrez cet écran depuis l'écran **Réseaux**, l'écran affiche l'identifiant SSID en haut.
- Les réseaux que le testeur n'a pas entendus récemment apparaissent en grisé si l'option **Griser points d'accès inaudibles** est activée (voir page 18).



: Le réseau utilise des périphériques ad hoc. Ces périphériques communiquent directement avec d'autres périphériques, et non pas en empruntant un point d'accès faisant partie du réseau. Les périphériques ad-hoc peuvent donner aux pirates un accès aux données échangées sur le réseau. (Certaines directives informatiques autorisent néanmoins les périphériques ad-hoc.)

[Caché] : Le réseau ne diffuse pas son identifiant SSID.

Si un SSID s'affiche entre crochets, le testeur a détecté le SSID caché dans les paquets d'autres clients sans fil. Dans AirCheck Manager, ces SSID s'affichent sans crochets.

⑦  : L'état de sécurité du point d'accès.



Cadenas ouvert rouge : La sécurité n'est pas activée pour le point d'accès.



Cadenas refermé jaune : Le point d'accès utilise le protocole de sécurité WEP.



Cadenas refermé vert : Tous les points d'accès utilisent un protocole de sécurité qui est plus sécurisé que WEP ; par exemple, WPA ou WPA2.



: Le point d'accès est un périphérique ad hoc. Ces périphériques communiquent directement avec d'autres périphériques, et non pas en empruntant un point d'accès faisant partie du réseau. Les périphériques ad-hoc peuvent donner aux pirates un accès aux données échangées sur le réseau. (Certaines politiques de réseau autorisent les périphériques ad hoc.)

(...) : Tous les points d'accès n'utilisent pas le même type de sécurité. Par exemple, certains utilisent WEP, d'autres WPA.

⑧ **802.11** : Normes 802.11 que le point d'accès utilise.



802.11a : Utilise la bande 5 GHz.



802.11b : Utilise la bande 2,4 GHz.



802.11g : Utilise la bande 2,4 GHz.



802.11n : Peut être utilisé dans les bandes 2,4 GHz ou 5 GHz.



Barres rouges : Le testeur a reçu un code de pays 802.11d du point d'accès. Le pays est différent du pays sélectionné dans l'option **Outils > Définir le pays** dans le testeur.

  : Les points d'accès qui utilisent la norme 802.11n peuvent coupler un canal à un canal d'extension au-dessus ( ou en dessous () pour former un canal 40 MHz. Ce canal plus large permet d'obtenir un meilleur débit réseau.

(...) : Les points d'accès n'utilisent pas tous la même norme 802.11.

- ⑨ **Notes (Remarques)** : Appuyez sur  pour atteindre le champ de notes. Le testeur ajoute des notes automatiquement. Voir page 35. Les points d'accès accompagnés de remarques sont violets.

(...) : Le point d'accès est accompagné de plusieurs remarques. Pour afficher toutes les remarques, allez à l'écran **Détails du point d'accès**.

- ⑩  : **Tri 1**, ordres de tri croissant et décroissant
  : **Tri 2**, ordres de tri croissant et décroissant

Pour trier la liste par ordre croissant ou décroissant, appuyez sur  et sur  pour sélectionner un en-tête de colonne, puis appuyez sur  ou  **Tri 1**. Par exemple, pour retrouver facilement le point d'accès avec le signal le plus fort, sélectionnez  en haut de la colonne, puis appuyez sur  ou  **Tri 1**. Le point d'accès avec le signal le plus fort est placé en haut de la liste.

Pour appliquer un ordre de tri secondaire, sélectionnez un autre en-tête de colonne, puis appuyez sur  **Tri 2**.

- ⑪ Appuyez sur  **Connexion** pour vous connecter au point d'accès sélectionné. Voir page 42.

Si le testeur ne peut pas se connecter au point d'accès sélectionné, le bouton indique « **Connexion*** ». Voir page 42.

Pour se connecter au point d'accès sécurisé, le testeur doit disposer d'un profil contenant des identifiants de sécurité. Voir page 14.

- ⑫  48 : Le canal surveillé actuellement par le testeur. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20

- ⑬  : Nombre de points d'accès que le testeur entend dans la zone ciblée. Si l'option **Regrouper points d'accès virtuels** est activée, ce nombre ne comprend pas les points d'accès virtuels. Voir page 18.

- ⑭ Appuyez sur  **ACL** pour modifier l'état d'autorisation du point d'accès mis en surbrillance. Voir page 17.

Pour afficher les détails sur un point d'accès, mettez celui-ci en surbrillance, puis appuyez sur . Voir figure 7.

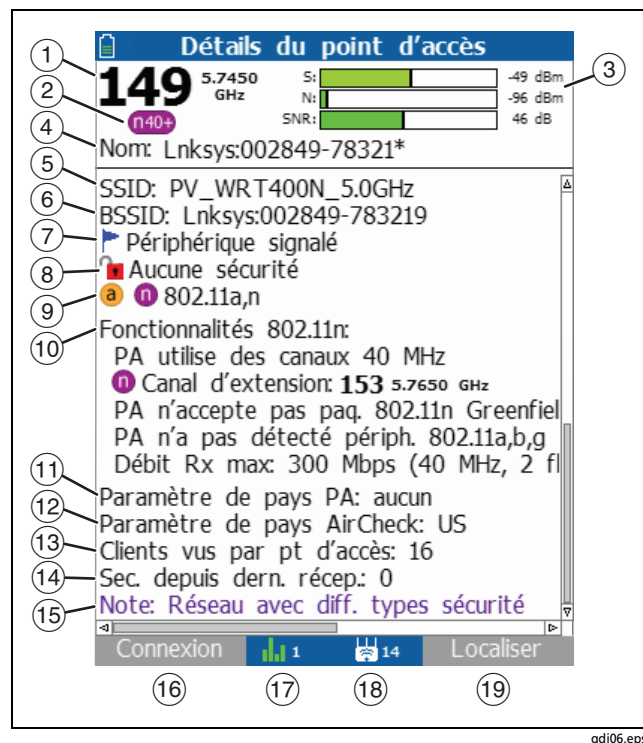


Figure 7. Ecran Détails du point d'accès

- ① Canal et fréquence du point d'accès. Le numéro est rouge si le canal est interdit dans le pays sélectionné sous **Outils > Définir le pays**.
- ② **n40+** **n40-**: Le canal principal (①) est couplé avec un canal d'extension au-dessus (**n40+**) ou en dessous (**n40-**) pour créer un canal de 40 MHz. Ce canal plus large permet d'obtenir un meilleur débit réseau. Le canal d'extension s'affiche sous **Fonctionnalités 802.11n** (⑩).
- ③ L'intensité du signal (**S**), l'intensité du bruit (**N**) et le rapport signal/bruit (**SNR**). Vous pouvez modifier les seuils des couleurs dans les affichages incrémentaux. Les barres sont grises si le testeur n'entend pas le point d'accès. Voir page 21.
- ④ **Nom** : Le nom du point d'accès, si un nom est inclus aux trames des balises et aux trames de réponses de sondage.
- ⑤ **SSID** : Identificateur SSID (Service Set Identifier). Le nom du réseau qui utilise les points d'accès.
- ⑥ **BSSID** : Identificateur SSID de base (Basic Service Set Identifier). L'adresse MAC du point d'accès.

Remarque

Certains points d'accès possèdent plusieurs adresses MAC pour leurs interfaces filaires et sans fil.

- ⑦ L'état d'autorisation du point d'accès.
- ⑧ L'état de sécurité du point d'accès.
- ⑨ Normes 802.11 que le point d'accès peut utiliser.
- ⑩ **Fonctionnalités 802.11n** : Remarques sur les points d'accès pouvant utiliser la norme 802.11n. Voir Tableau 4 à la page 36.
- ⑪ **Paramètre de pays PA** : Le code de pays que le point d'accès transmet. Si le **Paramètre de pays PA** n'est pas compatible avec le **Paramètre de pays AirCheck**, le point d'accès présente des barres rouges dans la colonne **802.11**. Voir « Fonctionnement 802.11d » à la page 20. L'annexe C indique les pays associés aux codes.
- ⑫ **Paramètre de pays AirCheck** : Code du pays sélectionné dans l'option **Outils > Définir le pays**. Voir « Fonctionnement 802.11d » à la page 20. L'annexe C indique les pays associés aux codes.
- ⑬ **Clients vus par pt d'accès** : Nombre de clients utilisant actuellement le point d'accès. « – » s'affiche si le point d'accès ne signale pas le nombre de clients qu'il contient.
- ⑭ **Sec. depuis dern. récep.** : Nombre de secondes écoulé depuis que le testeur a entendu le point d'accès.
- ⑮ Remarques sur le point d'accès. Voir Tableau 3 à la page 35.
- ⑯ Appuyez sur  **Connexion** pour vous connecter au point d'accès. Voir page 42.
Si le testeur ne peut se connecter au réseau sélectionné, le bouton indique « **Connexion*** ». Voir page 42.
- ⑰  **48** : Le canal actuellement surveillé par le testeur. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20
- ⑱  : Nombre de points d'accès que le testeur entend dans la zone ciblée. Si l'option **Regrouper points d'accès virtuels** est activée, ce nombre ne comprend pas les points d'accès virtuels. Voir page 17.
- ⑲ Appuyez sur  **Localiser** pour localiser le point d'accès. Voir page 54.

Si le testeur ne découvre pas de point d'accès

Dans certains cas, le testeur ne détecte aucun point d'accès :

- Le testeur ne peut pas entendre le point d'accès car vous êtes trop éloigné.
- Le point d'accès ne déclenche aucune balise lorsque le testeur écoute le canal utilisé par le point d'accès.
- Le testeur ne peut pas entendre le point d'accès car le signal n'est pas perceptible à travers un mur ou un autre obstacle.
- Les interférences sont trop importantes sur le canal utilisé par le point d'accès. Sélectionnez **Canaux** pour afficher les interférences provenant de sources non 802.11 sur le canal.

Remarques sur les réseaux et les points d'accès

Les tableaux 3 et 4 décrivent les remarques que le testeur peut ajouter aux réseaux et aux points d'accès.

Tableau 3. Remarques sur les réseaux et les points d'accès

Réseau ad hoc opérationnel	Ce SSID est un réseau ad hoc. Un ordinateur portable diffuse l'identifiant SSID car il s'est automatiquement connecté à un autre ordinateur portable qui a transmis l'identifiant SSID. Les périphériques ad-hoc peuvent donner aux pirates un accès aux données échangées sur le réseau. (Certaines directives informatiques autorisent néanmoins les périphériques ad-hoc.)
Le canal est interdit pour ce pays	Le point d'accès utilise un canal qui n'est pas autorisé dans le pays sélectionné sous Outils > Définir le pays . Vérifiez que le pays sélectionné sous Outils > Définir le pays est correct.
Interférences possibles — chevauchement des canaux standard	Le point d'accès utilise un canal dans la bande 2,4 GHz susceptible de chevaucher des canaux adjacents. Cela peut provoquer des interférences sur les canaux adjacents. <i>Remarque</i> <i>Aux Etats-Unis, les canaux sans chevauchement sont 1, 6 et 11.</i>
Réseau avec différents types sécurité	Tous les points d'accès associés à cet identifiant SSID n'utilisent pas le même type de sécurité.

-suite-

Tableau 3. Remarques sur les réseaux et les points d'accès (suite)

40 MHz 802.11n n'est pas recommandé sur 2,4 GHz	Vous devez coupler les canaux dans la bande 2,4 GHz car cette bande ne dispose que de trois canaux qui ne se chevauchent pas. Si vous couplez deux canaux, un seul canal est alors disponible pour les autres périphériques.
Pays inattendu au point d'accès	Le code de pays du points d'accès n'est pas compatible avec le pays sélectionné dans l'option Outils > Définir le pays du testeur.

Tableau 4. Fonctionnalités 802.11n (affichées sur l'écran Détails du point d'accès)

Le point d'accès (AP en anglais) utilise les canaux de 40MHz s'il le peut	Dans certains cas, le point d'accès n'utilise pas les canaux de 40 MHz. Exemples : • Le point d'accès a entendu d'autres points d'accès ou clients qui utilisent des canaux en chevauchement avec les canaux de 40 MHz. • Un client utilisant le point d'accès a entendu ces points d'accès ou clients et informé le point d'accès de ne pas utiliser les canaux de 40 MHz. Reportez-vous à la norme 802.11n lorsque les points d'accès ne peuvent pas utiliser les canaux de 40 MHz.
PA config. pr util. canaux 20MHz	L'utilisateur a défini le point d'accès (PA) pour qu'il n'utilise que les canaux de 20 MHz.
PA accepte paq. 802.11n Greenfield	Le point d'accès (PA) peut augmenter la vitesse s'il utilise des paquets Greenfield.

Tableau 4. Fonctionnalités 802.11n (affichées sur l'écran Détails du point d'accès) (suite)

PA n'accepte pas paq. 802.11n Greenfield	Le point d'accès (PA) n'accepte pas de paquets 802.11n Greenfield. L'utilisateur a informé le point d'accès de ne jamais utiliser de paquets Greenfield, ou le point d'accès entend des clients a, b ou g et ne fonctionne pas en mode Greenfield 802.11n.
PA a détecté périph. 802.11a,b,g	Le point d'accès (PA) doit utiliser la protection pour ne pas provoquer de conflits lors des transmissions a, b ou g. Les procédures de protection réduisent la vitesse du réseau 802.11n. • Le point d'accès a entendu les clients ou points d'accès 802.11a, b ou g. • Un client utilisant le point d'accès a entendu les clients ou points d'accès 802.11a, b ou g.
PA a détecté périph. 802.11a,b,g	Le point d'accès (PA) n'a pas besoin d'utiliser la protection pour empêcher les conflits avec les transmissions a, b ou g. Le point d'accès peut fonctionner à vitesse maximale.
Débit Rx max	Le débit en réception maximum pour le point d'accès à ce stade. Le débit peut évoluer à mesure que le point d'accès s'adapte aux modifications du trafic sans fil dans cette zone. • 20 MHz ou 40 MHz : La largeur de canal nécessaire pour obtenir le débit maximal. • Flux X : Nombre de flux de données que le point d'accès utilise pour obtenir le débit maximum. • 1/2 GI : Le point d'accès utilise un intervalle de protection court (400 ns au lieu de 800 ns) pour obtenir le débit maximal. Un intervalle de protection court permet ainsi d'augmenter le débit de 270 Mbps à 300 Mbps en réception.

Utilisation du canal

La fonction de l'utilisation du canal indique le volume de trafic sans fil sur chaque canal. Elle affiche également les interférences des sources non 802.11. La figure 8 présente l'écran **Utilisation du canal**.

Pour afficher les détails sur un canal (figure 9), utilisez   pour mettre en surbrillance le canal, puis appuyez sur .

Pour sélectionner les bandes associées à cette fonction, sélectionnez **Outils**, puis **Gérer les paramètres 802.11**. Voir le tableau 2 page 17.

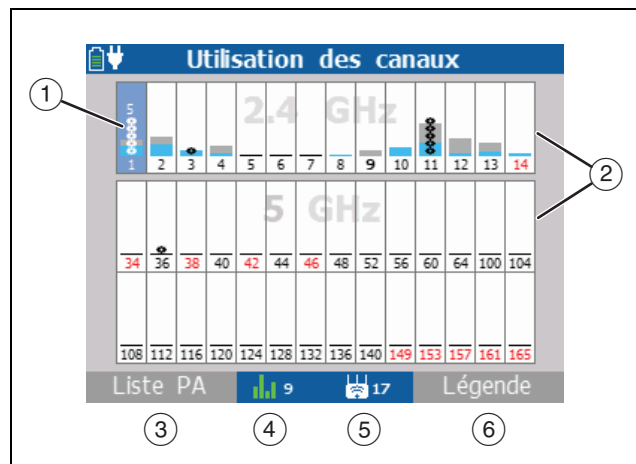


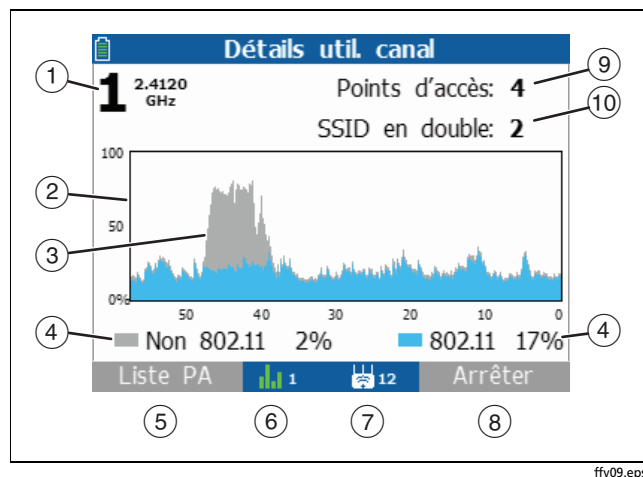
Figure 8. Ecran Utilisation du canal

- ① L'affichage incrémental indique la capacité du canal utilisée par les périphériques 802.11 (bleus) et par les périphériques non 802.11 (gris). Plus une barre sur l'affichage est grande, plus le canal est utilisé.
- Les anneaux dans les barres de l'affichage incrémental montre le nombre de points d'accès utilisant le canal. Lorsque vous mettez le canal en surbrillance, le nombre de points d'accès actif s'affiche au-dessus de l'affichage incrémental.

Les canaux qui n'ont pas de points d'accès peuvent afficher le taux d'utilisation 802.11 en raison du chevauchement des points d'accès sur les canaux adjacents.

- ② Par défaut, le testeur affiche les canaux sur les bandes 2,4 GHz et 5 GHz. Pour n'afficher qu'une seule bande, modifiez le paramètre sous **Outils > Gérer les paramètres 802.11**.
- ③ Appuyez sur  **Liste PA** pour afficher les points d'accès qui utilisent le canal mis en surbrillance.

- ④  48: Le canal surveillé actuellement par le testeur. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20
- ⑤  5: Nombre de points d'accès que le testeur entend dans la zone ciblée. Cette option affiche le nombre de points d'accès physiques si l'option **Regrouper points d'accès virtuels** est sélectionnée. Voir page 17.
- ⑥ Pour afficher la description des icônes de l'écran **Utilisation du canal**, appuyez sur  **Légende**.



- ① Le numéro du canal et la fréquence du canal surveillé. Le numéro est rouge si le canal est interdit dans le pays sélectionné sous **Outils > Définir le pays**.
Pour changer de canal, appuyez sur

- ② Graphique de l'utilisation 802.11 et des interférences non 802.11 du canal sélectionné dans le temps en secondes. Plus l'utilisation est importante, plus le canal est utilisé. Les canaux très utilisés peuvent ralentir le réseau ou affecter la connectivité
- ③ Interférence d'un four à micro-ondes.
- ④ **Non 802.11, 802.11** : Le pourcentage de signaux sur le canal ne provenant pas de périphériques 802.11 (gris) et provenant de périphériques 802.11 (bleus).
Le bruit non 802.11 peut provenir de différentes sources : fours à micro-ondes, téléphones sans fil, appareils Bluetooth®, détecteurs de mouvement, caméras sans fil et autres appareils sans fil. Ce bruit peut interférer avec les connexions ou les performances du réseau sans fil.
- ⑤ Appuyez sur **Liste PA** pour afficher les points d'accès qui utilisent le canal. Voir figure 6.
- ⑥ 48 : Le canal que le point d'accès utilise. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Les barres sont rouges si le testeur a reçu des codes de pays différents de deux ou plusieurs points d'accès. Voir « Fonctionnement 802.11d » à la page 20.

- ⑦  : Nombre de points d'accès que le testeur entend dans la zone ciblée. Cette option affiche le nombre de points d'accès physiques si l'option **Regrouper points d'accès virtuels** est sélectionnée. Voir page 18.
- ⑧ Appuyez sur  **Arrêter** pour éteindre l'écran.
- ⑨ **Points d'accès** : Nombre de points d'accès utilisant le canal. Cette option affiche le nombre de points d'accès physiques si l'option **Regrouper points d'accès virtuels** est sélectionnée. Voir page 18.
- ⑩ **SSID en double** : Nombre de points d'accès dans la même zone utilisant le même canal et prenant en charge le même réseau. Cette situation peut provoquer un conflit car les points d'accès peuvent interférer les uns avec les autres.

Vérification de la connectivité

Utilisez les tests de connectivité pour vérifier le fonctionnement de ces fonctions de réseau sans fil :

- Les clients peuvent se connecter au réseau.
- Les clients ont accès aux services du réseau (par exemple, DHCP, DNS et routeurs).
- Les clients peuvent communiquer avec d'autres périphériques dans un délai raisonnable.
- La plage de connectivité pour les clients est satisfaisante.

Les tests mesurent également les paramètres de performances qui indiquent si le réseau présente une anomalie.

Charger un profil qui comprend des identifiants de sécurité

Le testeur doit disposer des identifiants de sécurité appropriés pour se connecter à un réseau sécurisé. Les réseaux sécurisés présentent un cadenas fermé vert ou jaune ( ) dans la colonne de sécurité.

Pour entrer les identifiants de sécurité, utilisez AirCheck Manager et établissez un profil de configuration comprenant les identifiants de sécurité. Transférez ensuite le profil vers le testeur. Voir page 14.

Remarque

Ces identifiants de sécurité ne peuvent pas être créés ni modifiés sur le testeur. Vous devez utiliser AirCheck Manager pour les créer ou les modifier.

Pour charger un profil

- 1 Dans l'écran d'accueil, sélectionnez **Outils**, puis **Gérer les fichiers**.
- 2 Sélectionnez **Charger le profil**, mettez en surbrillance le profil approprié, appuyez sur , puis sur  **Charger**.

Se connecter à un réseau ou à un point d'accès

Le testeur peut se connecter à un réseau (SSID) ou à un point d'accès spécifié (BSSID) pour confirmer que le réseau ou le point d'accès est accessible aux clients sans fil.

Vous pouvez également utiliser le testeur pour vous connecter à un réseau sécurisé et vérifier que les identifiants de sécurité sont corrects.

Le testeur affiche les étapes de la procédure de connexion et fournit un journal des événements qui se sont produits (figures 10 et 11).

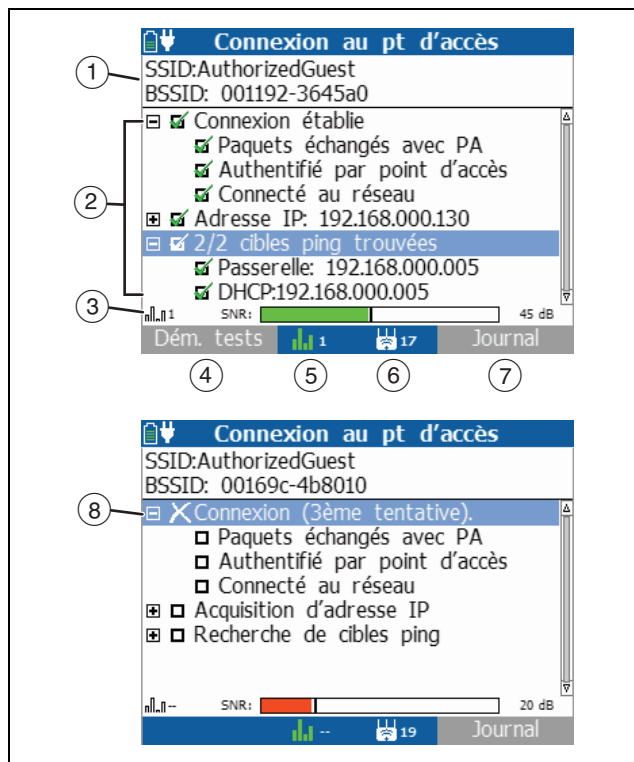
Si le testeur ne peut pas se connecter au réseau ou au point d'accès sélectionné, le bouton indique « **Connexion*** ». Cela se produit car le réseau utilise les identifiants de sécurité qui ne font pas partie du profil chargé.

Pour se connecter à un réseau

- 1 Si le réseau est sécurisé, vous devez charger un profil de configuration contenant les identifiants de sécurité pour le réseau. Voir page 14.
- 2 Dans l'écran d'accueil, sélectionnez **Réseaux**.
- 3 Mettez en surbrillance le réseau dans la liste **Réseaux (SSID)**, puis appuyez sur  **Connexion**.

Pour se connecter à un point d'accès spécifié

- 1 Si le point d'accès est sécurisé, vous devez utiliser un profil de configuration contenant les identifiants de sécurité pour ce point d'accès. Voir page 14.
- 2 Dans l'écran d'accueil, sélectionnez **Points d'accès**.
- 3 Sélectionnez un point d'accès dans la liste **Points d'accès**, puis appuyez sur  **Connexion**.



gdj04.eps

Figure 10. L'écran Connexion

① **SSID, BSSID** : Nom du réseau et adresse MAC du point d'accès que le testeur utilise pour la connexion. Lorsque l'utilisateur se connecte à un réseau, le testeur utilise normalement le point d'accès présentant le rapport signal/bruit le plus élevé. Si le réseau comprend des points d'accès sécurisés et non sécurisés, et si des identifiants sont disponibles pour la sécurité, le testeur essaie de se connecter au point d'accès sécurisé présentant le rapport signal/bruit le plus élevé. Certains réseaux utilisent un contrôleur pour assurer la connexion au point d'accès ayant le trafic le moins important.

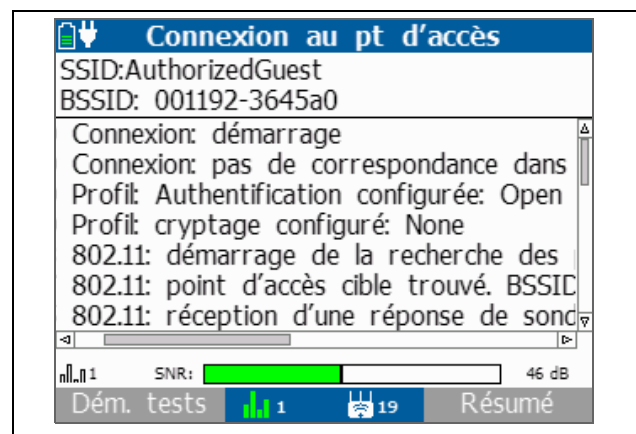
② Les étapes de la procédure de connexion. La liste associée à l'étape se réduit sur l'écran une fois l'étape terminée. Pour développer ou réduire la liste associée à une étape, mettez celle-ci en surbrillance, puis appuyez sur .

Dans le cadre des tests de connexion, le testeur émet un écho (ping) pour détecter les périphériques qui prennent en charge la connexion (les serveurs DHCP et DNS par exemple) et les adresses IP incluses au profil. Le testeur affiche une coche verte () si le périphérique a répondu, ou une croix rouge () s'il n'a pas répondu. Procédez à un test de détection ping pour détecter d'autres périphériques. Voir page 46.

- ③  **SNR** : Numéro du canal et le rapport signal/bruit du point d'accès. Vous pouvez modifier les seuils des couleurs dans les affichages incrémentaux. Voir page 21.
- ④ Appuyez sur  **Dém. tests** pour procéder à un test ping, et notamment le test **Portée connexion**.
- ⑤  **48** : Le canal que le point d'accès utilise. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20.
- ⑥  **5** : Nombre de points d'accès que le testeur entend dans la zone ciblée. Cette option affiche le nombre de points d'accès physiques si l'option **Regrouper points d'accès virtuels** est sélectionnée. Voir page 18.
- ⑦ Appuyez sur  **Journal** pour afficher des détails sur la procédure de connexion. Voir figure 11.
- ⑧ Connexion ayant échoué. Le testeur interrompt le processus de connexion après la troisième tentative. L'annexe A décrit les messages du journal signalant le moment de l'échec de la connexion.

Remarque

Sur l'écran du journal de connexion, appuyez sur  pour faire défiler la liste et afficher l'horodatage de chaque entrée du journal. Les horodatages sont présentés en secondes.



gdj10.bmp

Figure 11. Journal de connexion

Détecter un périphérique ou un serveur Web par commande ping

Vous pouvez entrer des adresses pour détecter d'autres périphériques ou serveurs Web par commandes ping. Cela permet de confirmer que les autres périphériques du réseau sont accessibles et de mesurer le temps de réponse.

- 1 Connectez-vous à un réseau ou à un point d'accès. Voir page 42.
- 2 Une fois la connexion terminée, appuyez sur  **Dém. tests.**

Sélectionnez une adresse IP dans la liste ou entrez une nouvelle adresse.

Pour entrer une nouvelle adresse

- a. Sélectionnez **Entrer l'adresse IP**.
- b. Utilisez   pour sélectionner la valeur à modifier.
- c. Utilisez   pour augmenter ou diminuer la valeur en surbrillance.
- d. Pour enregistrer l'adresse, appuyez sur  **Terminé.**

Remarque

Si vous enregistrez le profil, le testeur n'enregistre pas les adresses ping qui ont été saisies. Utilisez AirCheck Manager pour inclure dans un profil les adresses IP à la liste des adresses IP associées aux tests ping.

L'écran Ping (figure 12) affiche les résultats des tests ping. Pour utiliser une autre adresse pour la commande ping, appuyez deux fois sur , puis sélectionnez ou saisissez une autre adresse.

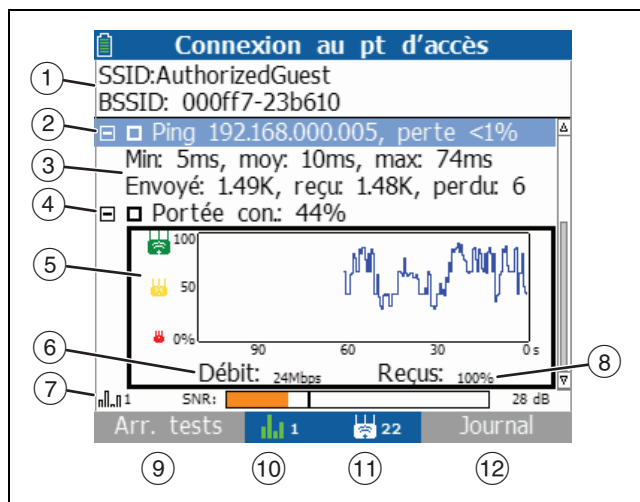


Figure 12. L'écran Ping

- ① **SSID, BSSID** : Nom du réseau et nom du point d'accès pour la cible de détection ping.
- ② **Commande Ping** : Adresse IP de la cible ping et pourcentage de réponses non reçues.

- ③ Les durées minimum (**min**), moyenne (**moy**) et maximum (**max**) des réponses ping du périphérique et le nombre de paquets envoyés, reçus et perdus pendant le test ping.
- ④ **Portée con** : La plage de connexion affiche la probabilité de la meilleure connexion possible avec le point d'accès à partir de l'emplacement de l'utilisateur. La meilleure connexion possible donne un pourcentage de réponses ping de 100% et le débit de données maximum possible. La valeur de la plage de connexion diminue à mesure que l'utilisateur s'éloigne du point d'accès. D'abord, le débit diminue. Lorsque l'utilisateur continue à s'éloigner du point d'accès, le pourcentage des réponses ping diminue et la connexion n'est plus fiable.

Le testeur utilise la formule suivante pour calculer la plage de connexion :

$$\text{pourcentage des réponses ping (⑧)} \times \left(\frac{\text{débit (⑥)}}{\text{débit maximum possible}} \right)$$

- ⑤ Graphique de la plage de connexion pour les 120 dernières secondes.
- ⑥ **Débit** : Le débit de transfert des données.

- ⑦  **SNR** : Le numéro du point d'accès et le rapport signal/bruit. Vous pouvez modifier les seuils des couleurs dans les affichages incrémentaux. Voir page 21.
- ⑧ **Reçus** : Le pourcentage de réponses ping (réponses pings reçues divisé par échos pings envoyés).
- ⑨ Appuyez sur  **Arr. tests** pour arrêter le test ping.
- ⑩  **48** : Le canal que le point d'accès utilise. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20
- ⑪  **5** : Nombre de points d'accès que le testeur entend dans la zone ciblée. Cette option affiche le nombre de points d'accès physiques si l'option **Regrouper points d'accès virtuels** est sélectionnée. Voir page 18.
- ⑫ Appuyez sur  **Journal** pour afficher des détails sur la procédure de connexion. Voir figure 11.

Détection des clients

Lorsque le testeur est allumé, il surveille sur chaque canal les trames de demande de sondage des clients du réseau. Pour afficher ces clients, utilisez la fonction **Répertoirer les clients**. Cette fonction vous indique si la carte d'interface du réseau d'un client peut transmettre des données. Elle indique également les informations sur le client, notamment les canaux qu'il utilise, ses débits binaires et les SSID qu'il utilise dans les vérifications.

L'écran Clients comprend une fonction **Localiser** qui permet de détecter les clients.

Lorsque la fonction **Répertoirer les clients** est utilisée, le testeur surveille chaque canal pendant plus longtemps que lorsque d'autres fonctions sont utilisées. Cela permet au testeur de détecter davantage de clients sur chaque canal.

Pour détecter les clients

Sélectionnez **Outils**, puis **Répertoirer les clients**. La figure 13 présente l'écran **Clients**.

Pour afficher les détails sur un client, mettez-le en surbrillance, puis appuyez sur . Voir figure 14.

Remarque

*Les informations les plus récentes sur le client s'affichent uniquement si ce dernier transmet des données pendant que le testeur surveille le canal utilisé. Pour recueillir les informations sur le client plus rapidement, sélectionnez **Outils > Gérer les paramètres 802.11**, puis activez une seule bande. Cela réduit le nombre de canaux que le testeur surveille.*

Ch	Signal	MAC	SSID	Mbps	Security	PA
1	-61	Fluke:02c412-a40017	[keepout]	54/1	🔒	cap-fp1-f21
1	-91	Apple:041e64-2ba6d9	[keepout]	5/1	🔒	cap-fp1-f21
1	-70	Intel:00516a-3d4b90	AuthorizedGuest	24/24	🔒	cap-fp1-f21
1	-66	Intel:0019f0-6eff48	---	48/5	--	001162-8645a0
1	-88	Intel:002717-ed0b90	---	6/2	--	001b45-b2cb52
1	-80	Fluke:05c017-a40418	---	11/1	--	001152-3645a8

⑧ ① ② ③ ④ ⑤ ⑥ ⑦

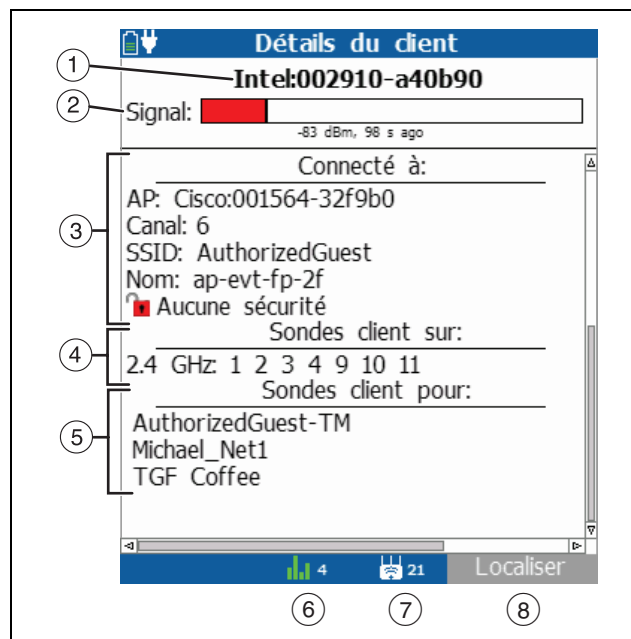
⑨ ⑩ ⑪

gdj12.eps

Figure 13. Ecran Clients

- ① **Ch** : Canal que le client utilise.
- ②  : L'intensité du signal. Vous pouvez modifier les seuils des couleurs dans les affichages incrémentaux. Voir page 21.
- ③ **MAC** : L'adresse MAC du client. L'adresse commence par le préfixe de l'abréviation du fournisseur, si ce préfixe est disponible. Se reporter à la section « oui_abbr.txt » page 64.
- ④ **SSID** : Identificateur SSID (Service Set Identifier). Le client est connecté à ce réseau.
[Caché] : Le réseau ne diffuse pas son identifiant SSID.
 Si un SSID s'affiche entre crochets, le testeur a détecté le SSID caché dans les paquets d'autres clients sans fil. Dans AirCheck Manager, ces SSID s'affichent sans crochets.
- ⑤ **Mbps** : Débits de transmission maximum et minimum déterminés par le testeur la dernière fois qu'il a surveillé le client.
- ⑥  : L'état de sécurité du point d'accès.
 Cadenas ouvert rouge : La sécurité n'est pas activée pour le point d'accès.
 Cadenas refermé jaune : Le point d'accès utilise le protocole de sécurité WEP.
-  Cadenas refermé vert : Tous les points d'accès utilisent un protocole de sécurité qui est plus sécurisé que WEP ; par exemple, WPA ou WPA2.
- ⑦ **PA** : Nom ou BSSID du point d'accès que le client utilise pour la connexion au réseau.
- ⑧  : **Tri 1**, ordres de tri croissant et décroissant
 : **Tri 2**, ordres de tri croissant et décroissant
 Pour trier la liste par ordre croissant ou décroissant, appuyez sur  et sur  pour sélectionner un en-tête de colonne, puis appuyez sur  ou  **Tri 1**. Par exemple, pour retrouver facilement le point d'accès avec le signal le plus fort, sélectionnez  en haut de la colonne, puis appuyez sur  ou  **Tri 1**. Le point d'accès avec le signal le plus intense est placé en haut de la liste.
 Pour appliquer un ordre de tri secondaire, sélectionnez un autre en-tête de colonne, puis appuyez sur  **Tri 2**.
- ⑨  48 : Le canal actuellement surveillé par le testeur. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20

- ⑩ : Nombre de points d'accès que le testeur entend dans la zone ciblée. Si l'option **Regrouper points d'accès virtuels** est activée, ce nombre ne comprend pas les points d'accès virtuels. Voir page 18.
- ⑪ Appuyez sur  **Localiser** pour localiser le client. Voir page 54.



gdj11.eps

Figure 14. Ecran Détails du client

- ① L'adresse MAC du client. L'adresse commence par le préfixe de l'abréviation du fournisseur, si ce préfixe est disponible. Se reporter à la section « oui_abbr.txt » page 64.
- ② **Signal** : Intensité du signal de la dernière transmission du client et heure à laquelle le testeur a entendu la transmission. Après 120 secondes, les secondes passent aux minutes. Après 120 minutes, les minutes passent aux heures.
- ③ **Connecté à** : Si le client est ou était connecté à un réseau ou a récemment tenté de s'y connecter, cette section présente des informations sur le point d'accès utilisé par le client. Si cette section indique uniquement le BSSID et le canal du point d'accès, il faut un temps plus long au testeur pour recueillir les informations.
- ④ **Sondes client sur** : Canaux que le client vérifie.
- ⑤ **Sondes client pour** : SSID que le client utilise pour procéder à la vérification. Quand un client se connecte à un réseau, il ne vérifie pas nécessairement l'ensemble des réseaux, de sorte que la liste n'indique pas toujours tous les SSID mis à la disposition du client. D'autres SSID s'affichent si le client se déplace.
- ⑥  48 : Le canal actuellement surveillé par le testeur. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20
- ⑦  5 : Nombre de points d'accès que le testeur entend dans la zone ciblée. Si l'option **Regrouper points d'accès virtuels** est activée, ce nombre ne comprend pas les points d'accès virtuels. Voir page 18.
- ⑧ Appuyez sur  **Localiser** pour localiser le client. Voir page 54.

Si le testeur ne détecte pas de client

Dans certains cas, le testeur ne découvre aucun client :

- La carte sans fil dans le client est désactivée.
- Le testeur ne peut pas entendre le client car l'utilisateur est trop éloigné du client.
- Le testeur ne peut pas entendre le client car le signal ne peut pas traverser un mur ou un autre obstacle.
- Les interférences sont trop importantes sur le canal utilisé par le client. Sélectionnez **Canaux** pour afficher les interférences provenant de sources non 802.11 sur le canal.
- Le testeur n'analyse pas la bande que le client utilise. Reportez-vous au paramètre sous **Outils > Gérer les paramètres 802.11**.
- Le client ne transmet pas la vérification lorsque le testeur écoute le canal utilisé par le client.

Localisation d'un point d'accès ou d'un client

- 1 Pour localiser un point d'accès : Sélectionnez **Réseaux** ou **Points d'accès**, puis utilisez  et  et  pour accéder à l'écran **Détails du point d'accès** associé au point d'accès à localiser.

Pour localiser un client : Sélectionnez **Outils**, puis **Répertoire des clients**. Utilisez  et  pour mettre en surbrillance le client à localiser.

- 2 Appuyez sur  **Localiser**. La figure 15 présente l'écran **Localiser point d'accès**. La figure 16 présente l'écran **Emplacement du client**.
- 3 Divisez la zone à explorer en quatre quadrants conformément à la figure 17. Allez dans un coin de cette zone.
- 4 Notez l'intensité du signal.
- 5 Dirigez-vous vers les trois autres coins de la zone et notez l'intensité du signal à chaque angle.
- 6 Dirigez-vous vers le premier coin de la section présentant le signal le plus intense.
- 7 Répétez les étapes 4, 5 et 6 jusqu'à ce que le point d'accès ou le client soit localisé.

Remarques

Si vous ne détectez pas le point d'accès ou le client, examinez les surfaces au-dessus et en dessous de vous.

Si un client reste introuvable alors qu'il indique la présence d'une connexion au réseau, commencez par détecter le point d'accès qu'il utilise, puis recherchez le client.

Dans les grandes zones ouvertes, l'antenne externe disponible en option permet de localiser les points d'accès plus rapidement. Voir page 58.

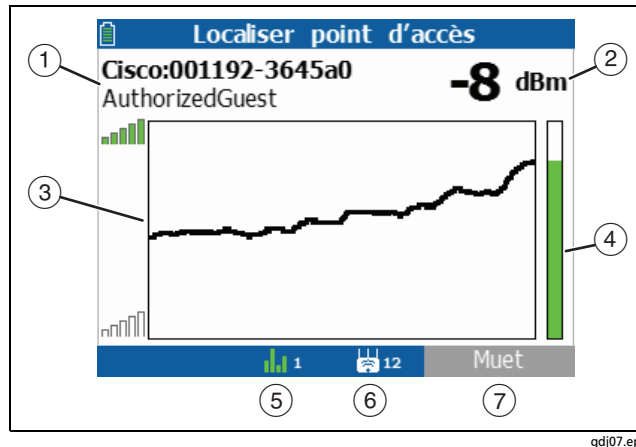


Figure 15. Ecran Localiser point d'accès

- ① Nom du réseau (SSID) et adresse MAC du point d'accès (BSSID).
- ② L'intensité du signal provenant du point d'accès. L'écran affiche « — » si le testeur n'entend pas le point d'accès.
- ③ Graphique de l'intensité du signal dans le temps. Si le testeur n'entend pas le point d'accès, la ligne ne s'affiche pas.
- ④ Jauge graphique indiquant l'intensité du signal à l'heure actuelle. La barre est grise si le testeur n'entend pas le point d'accès.
- ⑤ 48: Le canal que le point d'accès utilise. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20
- ⑥ 12: Nombre de points d'accès que le testeur a détecté. Si l'option **Regrouper points d'accès virtuels** est activée, ce nombre ne comprend pas les points d'accès virtuels. Voir page 17.
- ⑦ Appuyez sur **Muet** pour désactiver le son.

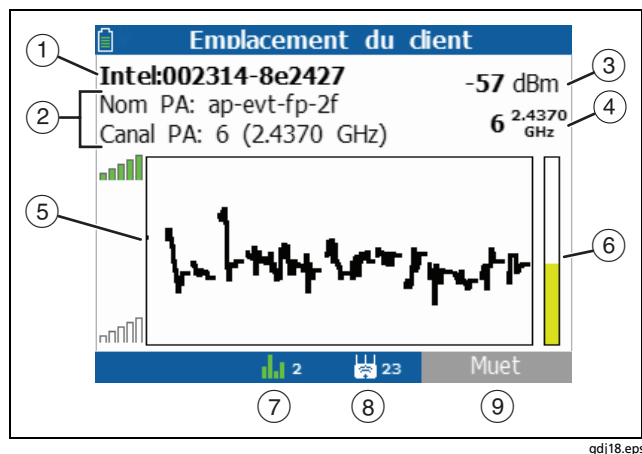


Figure 16. Ecran Emplacement du client

- ① L'adresse MAC du client. L'adresse commence par le préfixe de l'abréviation du fournisseur, si ce préfixe est disponible. Se reporter à la section « oui_abbr.txt » page 64.
- ② Nom, canal et fréquence du point d'accès que le client utilise pour la connexion au réseau.
- ③ Intensité du signal provenant du client. L'écran affiche « — » si le testeur n'entend pas le client.

- ④ Canal le plus surveillé par le testeur. Il s'agit du canal que le client a utilisé la dernière fois que le testeur a entendu le client. Le testeur surveille ce canal pendant 2 secondes, surveille un autre canal pendant 1 seconde, puis surveille de nouveau le premier canal pendant 2 secondes. Si le client change de canal, le testeur retrouve le client sur le nouveau canal après un certain temps.

Pour modifier ce canal, appuyez sur . Le testeur surveille le nouveau canal pendant 2 secondes et continue de surveiller les autres canaux comme avant.

- ⑤ Graphique de l'intensité du signal dans le temps. Si le testeur n'entend pas le client, la ligne ne s'affiche pas.
- ⑥ Jauge graphique indiquant l'intensité du signal à l'heure actuelle. La barre est grise si le testeur n'entend pas le client.

- ⑦ 48: Canal surveillé actuellement par le testeur. Voir ④.

La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Voir « Fonctionnement 802.11d » à la page 20

- ⑧ 5: Nombre de points d'accès que le testeur a détecté. Si l'option **Regrouper points d'accès virtuels** est activée, ce nombre ne comprend pas les points d'accès virtuels. Voir page 17.

- ⑨ Appuyez sur **Muet** pour désactiver le son.



57

L'antenne directionnelle externe

Dans les grands espaces ouverts, l'antenne directionnelle externe peut afficher la direction de la source d'un signal plus précisément que l'antenne omnidirectionnelle du testeur.

Remarque

Dans les zones comptant beaucoup de salles (établissements scolaires ou hospitaliers notamment), l'antenne omnidirectionnelle interne permet de localiser les points d'accès.

Pour localiser un point d'accès en utilisant l'antenne externe

- 1 Branchez l'antenne à la fiche d'antenne derrière le testeur. L'écran affiche l'icône de l'antenne () lorsque cette dernière est branchée. Le testeur n'utilise que l'antenne externe lorsque l'antenne est connectée.

Remarque

Lorsque l'antenne externe est connectée, le testeur ne transmet pas ; il ne se connecte donc pas à un réseau ou à un point d'accès.

- 2 Divisez la zone en quatre quadrants conformément à la figure 18. Dirigez-vous vers le centre de la zone.
- 3 Pour localiser un point d'accès : Sélectionnez **Réseaux** ou **Points d'accès**, puis utilisez  et  pour accéder à l'écran **Détails du point d'accès** associé au point d'accès à localiser.

Pour localiser un client : Sélectionnez **Outils**, puis **Répertorier les clients**. Utilisez  pour mettre en surbrillance le client à localiser.

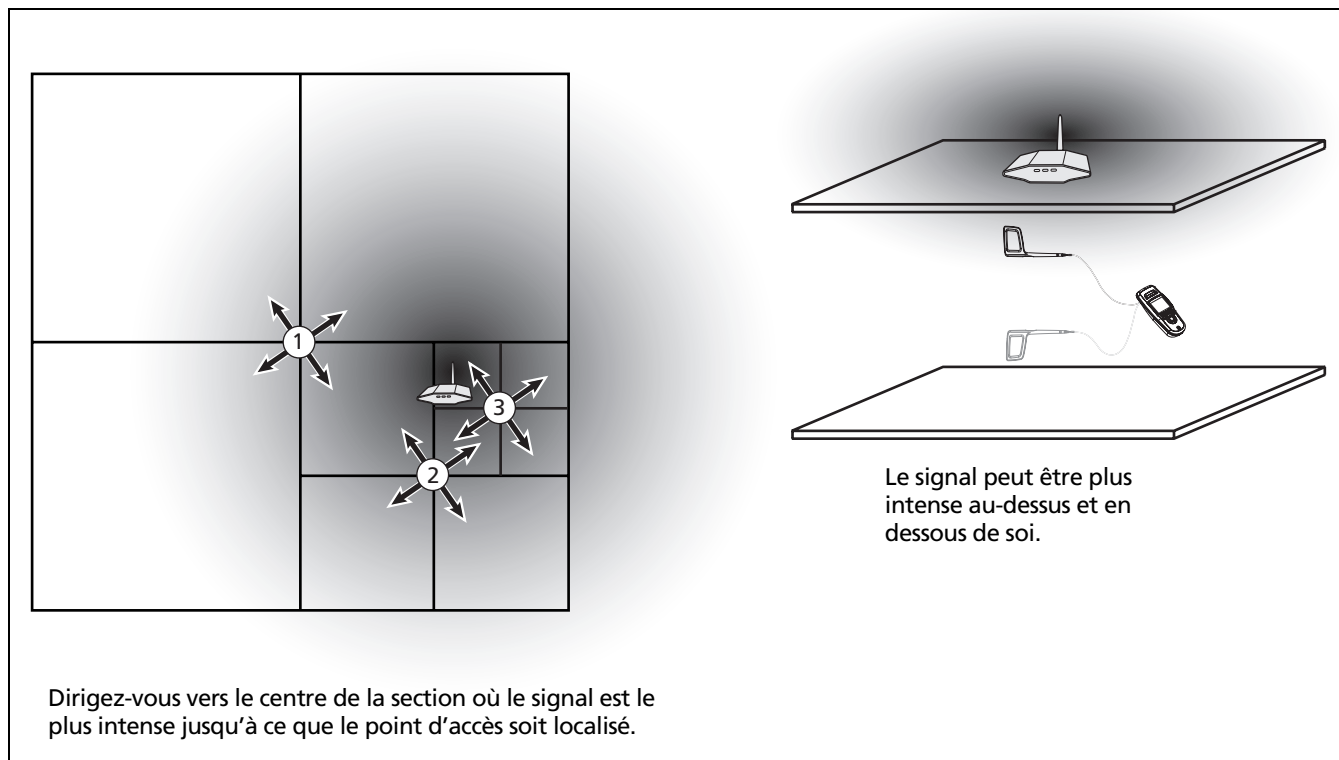
- 4 Appuyez sur  **Localiser**.
- 5 Dirigez l'antenne vers chaque coin de la zone. La figure 19 montre comment orienter l'antenne.
- 6 Dirigez-vous vers le centre de la section montrant le signal le plus intense.
- 7 Répétez les étapes 2, 5 et 6 jusqu'à ce que le point d'accès ou le client soit localisé.

Remarque

Si vous ne détectez pas le point d'accès ou le client, examinez les surfaces au-dessus et en dessous de vous.

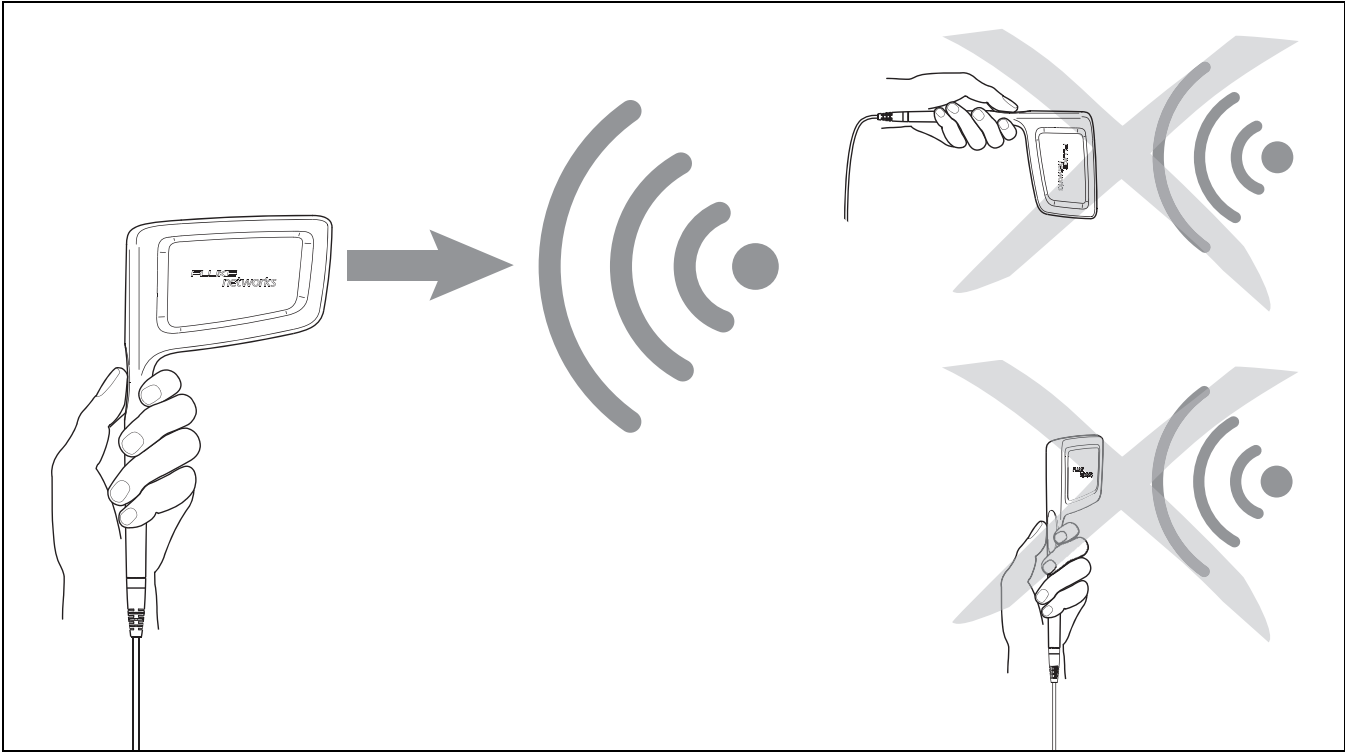
Respectez ces directives en utilisant l'antenne externe :

- Maintenez l'antenne à une hauteur constante. Vous pouvez obtenir des mesures plus stables si vous maintenez l'antenne au-dessus des murs des bureaux à cloisons.
- Ne bougez pas le bras en pointant l'antenne dans les différentes directions. Maintenez le testeur et l'antenne dans la même position tout en tournant sur vous-même.



ffy17.eps

Figure 18. Schéma de recherche de l'antenne externe



ffy13.eps

Figure 19. Comment orienter l'antenne externe

Réglage des mesures d'intensité du signal en fonction des autres périphériques

Les mesures d'intensité du signal prises par d'autres modèles de testeurs sans fil ou par des clients utilisés comme point de référence peuvent diverger. Ces différences sont essentiellement dues aux antennes. Afin d'harmoniser les périphériques, vous pouvez ajouter un décalage aux mesures AirCheck.

Pour ajouter un décalage aux mesures d'intensité du signal

1 Déterminez la valeur de décalage :

Utilisez le testeur AirCheck et les autres périphériques pour mesurer l'intensité du signal au même emplacement. Prenez note de la différence des mesures pour chaque canal qui vous importe.

2 Sélectionnez **Outils**.

- 3 Sélectionnez **Gérer les paramètres 802.11**, puis **Utiliser réglage de signal pers.**
- 4 Dans l'écran **Décalages utilisateur**, utilisez  pour sélectionner un canal, puis  pour choisir une valeur de décalage.
- 5 Répétez l'étape 4 pour les autres canaux si nécessaire.
- 6 Pour enregistrer les valeurs de décalage, appuyez sur  **Enregistrer**.

Lorsque l'utilisateur éteint son testeur, les valeurs de décalage sont enregistrées dans le profil. Ces valeurs de décalage s'affichent également dans les rapports générés dans AirCheck Manager.

Avertissement

Par la suite, gardez bien à l'esprit que vous avez réglé les décalages afin d'éviter les mesures incohérentes.

Enregistrement d'une session de tests

Pour enregistrer les informations que le testeur a recueillies depuis qu'il est sous tension ou depuis le dernier enregistrement d'une session, appuyez sur  ou débranchez le câble USB. Une session comprend les informations suivantes :

- Informations de réseau, point d'accès, client et canal (graphiques exclus)
- Liste de clients ayant transmis les sondages
- Résultats de la dernière connexion établie
- Résultats du dernier test ping
- Journal de connexion

Pour enregistrer les données d'une session de tests

- 1 Appuyez sur . Le testeur affiche un nom de fichier séquentiel par défaut en bas de l'écran.
 - Pour enregistrer la session sous le nom de fichier affiché, appuyez sur  **Enregistrer**. Le testeur enregistre la session dans le dossier « SESSIONS ».
 - Pour remplacer une session de tests enregistrée sur le testeur, mettez en surbrillance la session, appuyez sur , sur  **Enregistrer**, puis sur  **OK**.

- Pour modifier le nom du fichier, appuyez sur  **Modifier**.

Remarque

Les noms de sessions sont limités à 8 caractères avec une extension de 3 caractères maximum.

L'extension doit être « .ACS » pour afficher la session dans AirCheck Manager.

- Pour supprimer des caractères du nom du fichier, appuyez sur  **Supprimer**.
- Pour ajouter des caractères au nom de fichier, utilisez   pour mettre en surbrillance un caractère, puis appuyez sur .
- Pour déplacer le curseur dans le nom de fichier, mettez le nom de fichier en surbrillance, puis appuyez sur  .
- Pour enregistrer la session à l'aide du nom de fichier modifié, appuyez sur  **Terminé**, puis sur  **Enregistrer**.

Pour afficher le fichier de session, ouvrez-le dans AirCheck Manager. Voir page 65.

Gestion des fichiers sur le testeur

Pour renommer un fichier

- 1 Sélectionnez **Outils**, puis **Gérer les fichiers**.
- 2 Sélectionnez **Renommer le fichier**.
- 3 Mettez un fichier en surbrillance, puis appuyez sur .
- 4 Pour modifier le nom du fichier, appuyez sur  **Modifier**.

Remarque

Les sessions doivent avoir l'extension « .ACS » et les profils doivent avoir l'extension « .ACP » pour être affichés dans AirCheck Manager.

- Pour supprimer des caractères du nom du fichier, appuyez sur  **Supprimer**.
- Pour ajouter des caractères au nom de fichier, utilisez  pour mettre en surbrillance un caractère, puis appuyez sur .
- Pour déplacer le curseur dans le nom de fichier, mettez le nom de fichier en surbrillance, puis appuyez sur .

- 5 Pour renommer le fichier par le nom créé, appuyez sur  **Terminé**, puis sur  **Renommer**.

Pour supprimer un fichier

- 1 Sélectionnez **Outils**, puis **Gérer les fichiers**.
- 2 Sélectionnez **Supprimer le fichier**.
- 3 Mettez un fichier en surbrillance, puis appuyez sur .
- 4 Appuyez sur  **Supprimer**.

Remarque

Si vous supprimez ou renommez un fichier nécessaire au fonctionnement du testeur, ce dernier recrée ce fichier lors de sa remise sous tension. Ce n'est pas le cas pour les profils créés, les fichiers de sessions enregistrés ou pour le fichier OUI_ABBR.TXT. Voir « A propos des fichiers sur le testeur » à la page 64.

Pour afficher la quantité d'espace disponible en mémoire

Utilisez le câble USB fourni avec le testeur pour relier le testeur au PC et utilisez l'une des procédures suivantes :

- Ouvrez AirCheck Manager, sélectionnez **Outils > Gestionnaire de profils**, puis consultez le graphique **Mémoire utilisée**.
- Utilisez le navigateur de fichiers dans le système d'exploitation du PC pour afficher la quantité d'espace mémoire disponible sur le testeur.

Si la mémoire est saturée, le testeur affiche **Mémoire saturée** lorsque vous tentez d'enregistrer un fichier.

A propos des fichiers sur le testeur

Le testeur enregistre les données au format XML (Extensible Markup Language). Les données des fichiers XML incluent des balises d'identification. Le logiciel lit les balises qu'utilisent les données. Un navigateur Web capable de lire ces balises peut ainsi afficher les fichiers XML sur une page Web.

Le testeur crée les types de fichiers XML suivants (noms de fichier par défaut) :

- **DEVICE.XML** : Ce fichier contient les informations qui s'affichent lorsque vous sélectionnez **Outils > Afficher les informations sur AirCheck**.

- **CURRENT.ACP** : Ce fichier contient une copie du profil actuel. Il contient également les modifications apportées aux paramètres du testeur depuis l'enregistrement ou le chargement du profil.
- **SNXXXXXX.ACS** : Les fichiers de sessions contiennent les informations sur les réseaux sans fil. Voir « Localisation d'un point d'accès ou d'un client » à la page 54 ». AirCheck Manager utilise des fichiers de sessions pour créer les rapports des sessions.

Le fichier texte **OUI_ABBR.TXT** contient les abréviations des noms des fabricants de périphériques d'interfaces pour réseaux. Le testeur utilise ces abréviations comme préfixes pour les adresses MAC.

Pour charger la dernière liste des préfixes de fournisseurs dans le testeur

- 1 Lancez la dernière version d'AirCheck Manager sur le PC et reliez le testeur au PC.
- 2 Sélectionnez **AirCheck > Mise à jour du logiciel**, puis l'onglet **Fichier de préfixe MAC de fournisseur**.
- 3 Cliquez sur **Mise à jour du fichier**, sélectionnez le fichier de préfixe (**oui_abbr.txt**), puis cliquez sur **Ouvrir**.

Si une liste plus récente que celle incluse avec la dernière version de AirCheck Manager est disponible sur le site Web de Fluke Networks, copiez-la vers le dossier « VendorPrefix » d'AirCheck Manager. Procédez ensuite conformément aux étapes fournies ci-dessus pour charger la liste dans le testeur.

Transférer les fichiers vers un PC

Pour utiliser AirCheck Manager et examiner les sessions de tests ou les profils enregistrés sur le testeur

- 1 Installez la dernière version du logiciel AirCheck Manager sur votre ordinateur. Démarrez le logiciel.
- 2 Mettez le testeur sous tension.
- 3 Utilisez le câble USB fourni avec le testeur pour relier le testeur au PC. La fenêtre AirCheck affiche les fichiers de sessions présents sur le testeur.

Pour afficher les profils présents sur le testeur, sélectionnez **Outils > Gestionnaire de profils** dans la barre d'outils AirCheck Manager.

Pour transférer les fichiers avec le système d'exploitation du PC

- 1 Mettez le testeur sous tension.
- 2 Utilisez le câble USB fourni avec le testeur pour relier le testeur au PC. Le système d'exploitation du PC affiche le testeur en tant qu'unité de disque.
- 3 Utilisez le système d'exploitation du PC pour copier les fichiers du testeur vers une unité de disque du PC.

Entretien

Avertissement

Pour éviter les risques d'incendie ou d'électrocution, les blessures ou l'endommagement du testeur :

- N'ouvrez pas le boîtier. Ce boîtier ne contient aucune pièce réparable ou remplaçable par l'utilisateur.
- Utilisez uniquement des pièces de rechange approuvées par Fluke Networks.
- Si vous remplacez des pièces qui ne sont pas indiquées comme étant des pièces de rechange, la garantie ne s'applique pas à ce produit et il peut être dangereux de l'utiliser.
- Utilisez uniquement des centres de service approuvés par Fluke Networks.

Nettoyer le testeur

Nettoyez l'écran à l'aide d'un nettoyant pour objectif et d'un chiffon doux et non pelucheux. Nettoyez le boîtier à l'aide d'un chiffon doux et humide, ou avec de l'eau et du savon doux.

Avertissement

Pour éviter d'endommager l'écran ou le boîtier, n'utilisez pas de solvants ou de matériaux abrasifs.

Mettre à jour le logiciel dans le testeur

- 1 Téléchargez le fichier de mise à jour du logiciel AirCheck sur le site Internet de Fluke Networks ou contactez Fluke Networks pour obtenir la mise à jour par une autre méthode. Enregistrez le fichier sur votre disque dur.
- 2 Téléchargez la dernière version d'AirCheck Manager sur le site Web de Fluke Networks.
- 3 Lancez AirCheck Manager sur votre ordinateur.
- 4 Mettez le testeur sous tension.
- 5 Utilisez le câble USB fourni avec le testeur pour relier le testeur au PC.

- 6 Dans AirCheck Manager, sélectionnez **AirCheck > Mise à jour du logiciel**.
- 7 Cliquez sur **Sélectionner**, mettez le fichier de mise à jour en surbrillance (extension .xlf), puis cliquez sur **Ouvrir**.
- 8 Cliquez sur **Mise à jour**.
- 9 Une fois le transfert terminé, débranchez le câble USB du testeur.
- 10 L'écran du testeur est vierge et le testeur affiche des repères pendant l'installation du fichier de mise à jour. Une fois la mise à jour terminée, l'écran d'accueil s'affiche sur le testeur.

Remarque

La touche d'alimentation est désactivée pendant la mise à jour du logiciel. Si vous retirez la batterie avant la fin de la mise à jour, celle-ci recommence au redémarrage du testeur.

Restaurer aux réglages d'usine

L'annexe B fournit la liste des paramètres par défaut destinés au testeur.

Pour restaurer les paramètres d'usine par défaut

- 1 Dans l'écran d'accueil, sélectionnez **Outils, Restaurer aux réglages d'usine**, puis appuyez sur  **OK**.
- 2 Pour terminer l'opération, appuyez sur , puis allumez le testeur.

Informations sur le périphérique

Pour afficher les informations sur le testeur

Dans l'écran d'accueil, sélectionnez **Outils**, puis **Afficher les informations sur AirCheck**.

- **Numéro de série** : Le numéro de série est également affiché sous le bloc-batterie.
- **Adresse MAC** : Adresse de contrôle d'accès au support (Media Access Control). L'adresse unique du testeur.
- **Version logicielle** : Version du logiciel du testeur.
- **Version USB** : Version du pilote USB du testeur.
- **Version Radio** : Version de la radio du testeur.

Si le testeur ne s'éteint pas

Si le testeur ne s'éteint pas, maintenez ⓘ enfoncé pendant environ 5 secondes.

Si le testeur ne s'éteint toujours pas, retirez puis réinstallez le bloc-batterie.

Options et accessoires

Le tableau 5 affiche les options et les accessoires proposés pour le testeur Wi-Fi AirCheck.

Pour obtenir la liste complète d'options et d'accessoires, visitez le site Web de Fluke Networks à l'adresse www.flukenetworks.com/fr.

Tableau 5. Options et accessoires

Option ou accessoire	N° de modèle Fluke Networks
Antenne directionnelle externe munie d'un connecteur RSMA	EXTANT-RPSMA
Bloc-batterie au lithium-ion pour le testeur AirCheck	WBP-LION
Détecteur PoE	POE-DETECTOR
Adaptateur/chargeur se branchant à un allume-cigare automobile	MS-Auto-Chg
Adaptateur secteur/chargeur, universel, 120 à 240 V c.a.	DTX-ACUN

Caractéristiques techniques

Caractéristiques ambiantes

Température de fonctionnement et humidité relative	0 °C à +45 °C (32 °F à 113 °F) <i>Remarque</i> <i>La batterie ne se charge pas si la température interne du testeur est supérieure à 45 °C (113 °F).</i>
Humidité de fonctionnement relative (% HR sans condensation)	90 % (10 °C à 35 °C ; 50 °F à 95 °F) 75 % (35 °C à 45 °C ; 95 °F à 113 °F)
Température d'entreposage	-20 °C à +60 °C (-4 °F à 140 °F)
Chocs et vibrations	aléatoires, 2 g, 5 Hz à 500 Hz (classe 2), chute d'un mètre
Sécurité	EN 61010-1 2e édition
Altitude	4 000 m ; Stockage : 12 000 m
Compatibilité électromagnétique (CEM)	FCC article 15 Classe A, EN 61326-1

Certifications et conformité	 Conforme aux directives de l'Union européenne
	 Conforme aux normes australiennes
	 Classé par la Canadian Standards Association (organisme normatif canadien)
	 Conforme aux réglementations FCC, articles 15.107, 15.109
	 ANATEL 1572-10-5988 (01)07898941652029 Certifié par la Agência Nacional de Telecomunicações (Anatel)

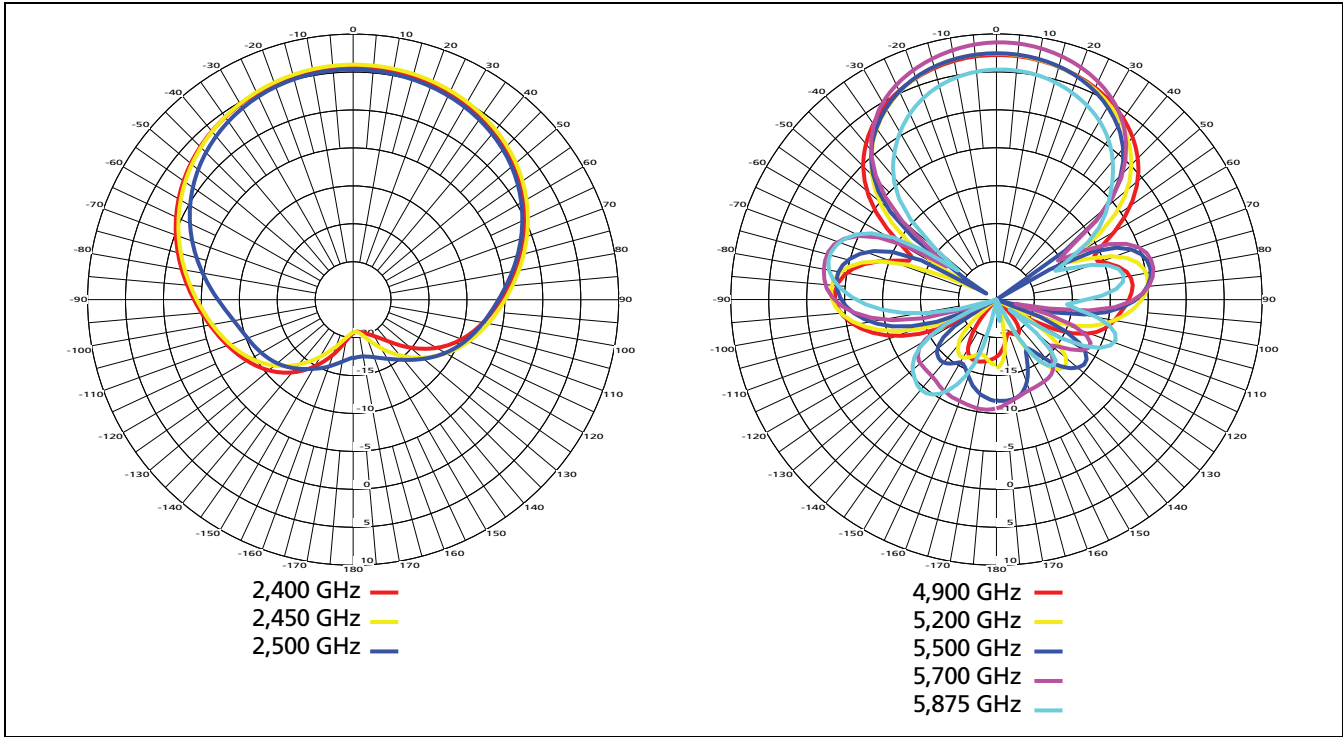
Caractéristiques générales

Dimensions	8,9 cm x 19,8 cm x 4,8 cm (3,5 x 7,8 x 1,9 pouces)
Poids	0,4 kg (14 onces)
Batterie	Bloc-batterie au lithium-ion amovible, rechargeable (18,5 watts/h)
Durée de vie	L'autonomie typique est de 5,5 heures. Le temps de charge typique est de 3 heures.
Adaptateur secteur/chargeur externe	Entrée CA : puissance d'entrée de 90 à 264 V CA, 48 à 62 Hz Sortie CC : 15 V CC à 1,2 A
Affichage	Ecran LCD couleur de 2,8 pouces (320 x 240 pixels)
Clavier	12 touches, élastomère
Témoins	2 témoins lumineux (indicateurs de transmission et de liaison)
Interface hôte	USB 5 broches mini-B
Antenne sans fil	Interne
Port d'antenne externe	Entrée uniquement. Connecteur SMA à polarité inverse.

Caractéristiques de l'accès sans fil

Conformité des caractéristiques	IEEE 802.11a, 11b, 11g, 11n
Fréquences de fonctionnement <i>Remarque</i> <i>Il s'agit des fréquences centrales des canaux prises en charge par le testeur AirCheck.</i>	Fréquences de canal en réception <i>Remarque</i> <i>Le testeur reçoit sur toutes les fréquences dans chaque pays.</i> Bande 2,4 GHz : 2,412 GHz à 2,484 GHz (canal 1 à canal 14) Bande 5 GHz : 5,170 GHz à 5,320 GHz, 5,500 GHz à 5,700 GHz, 5,745 GHz à 5,825 GHz (canaux 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165) Fréquences de canal en transmission <i>Remarque</i> <i>Le testeur transmet uniquement sur les fréquences autorisées dans le pays où il est utilisé.</i> Bande 2,4 GHz 802.11b : 2,412 GHz à 2,484 GHz (canal 1 à canal 14) 802.11g/n, bande passante 20 MHz (HT20) : 2,412 GHz à 2,472 GHz (canal 1 à canal 13) 802.11n, bande passante 40 MHz (HT40) : 2,422 GHz à 2,462 GHz (inclut toutes les combinaisons de paires de canaux couplés autorisées)

	Fréquences de canal en transmission (suite) Bande 5 GHz 802.11a/n, bande passante 20 MHz (HT20) : 5,180 GHz à 5,320 GHz, 5,500 GHz à 5,700 GHz, 5,745 GHz à 5,825 GHz (canaux 36, 40, 44, 48, 52, 56, 60, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165) 802.11n, bande passante 40 MHz (HT40) : 5,190 GHz à 5,310 GHz, 5,510 GHz à 5,670 GHz, 5,755 GHz à 5,795 GHz (inclut toutes les combinaisons de paires de canaux couplés autorisées)
Domaine réglementaire	Mode mondial, compatible 802.11d
Antenne directionnelle externe	
Fréquences	Plage de fréquences de 2,4 à 2,5 GHz et de 4,9 à 5,9 GHz
Connecteur	Gain minimal de 5 dBi sur la bande 2,4 GHz et de 7 dBi sur la bande 5 GHz Connecteur SMA à polarité inversée



ffy20.eps

Figure 20. Schémas de l'antenne externe (magnitude (dBi)) ou azimut (degrés)

Déclaration sur les interférences de la Federal Communication Commission des Etats-Unis et de Industrie Canada

Cet appareil a été testé et est certifié conforme aux limites définies pour un appareil numérique de classe B, en vertu de l'article 15 des réglementations FCC et IC. Ces limites ont pour objectif d'assurer une protection adéquate contre les interférences dangereuses dans les lieux d'habitation. Cet appareil produit, utilise et peut émettre des fréquences radioélectriques ; si son installation et son utilisation ne sont pas rigoureusement conformes aux consignes du constructeur, il risque de créer des parasites sur les récepteurs de radio et de télévision. L'absence de parasites sur la réception de radio et de télévision n'est toutefois pas garantie pour une installation particulière. Cet appareil peut perturber la réception d'un poste de radio ou de télévision. Ceci peut être vérifié en allumant puis en éteignant l'appareil. Nous vous recommandons d'essayer de remédier au problème à l'aide des mesures suivantes :

- réorientez ou déplacez l'antenne de réception ;
- éloignez l'appareil du récepteur ;
- branchez l'appareil et le récepteur sur des prises différentes ;

- consultez votre fournisseur ou un technicien en radio/télévision agréé.

Mise en garde FCC : Toute modification non autorisée par les autorités de la conformité peut entraîner la révocation du droit d'utilisation de ce produit.

Cet appareil est conforme à l'article 15 des réglementations FCC et IC. Son fonctionnement est tributaire des deux conditions suivantes :

(1) Cet appareil ne doit pas provoquer de parasites, et (2) il doit pouvoir accepter les interférences reçues, y compris les interférences susceptibles d'entraîner un fonctionnement indésirable.

Remarque importante : Déclaration FCC et IC sur l'exposition aux rayonnements

Cet appareil est conforme aux limites d'exposition aux rayonnements définies par la FCC et IC pour un environnement non commandé. L'emplacement et l'utilisation de cet appareil doivent respecter une distance minimale de 20 cm entre l'antenne et le corps de l'utilisateur.

Cet émetteur ne doit pas être situé dans la même pièce ou être utilisé avec une autre antenne ou émetteur.

Dans la bande 5,15 GHz à 5,25 GHz l'appareil n'est autorisé que pour l'utilisation à l'intérieur de locaux.

Certains canaux et/ou bandes de fréquences opérationnelles ne sont pas accessibles à l'utilisateur final et leur disponibilité varie selon les pays.

Déclaration de conformité de l'Union européenne (UE)

Cet appareil est en conformité avec les exigences essentielles de la directive R&TTE 1999/5/CE. Les méthodes de test suivantes ont été appliquées pour confirmer la présomption de conformité aux exigences essentielles de la directive R&TTE 1999/5/CE :

- **EN60950-1 : 2001 A11 : 2004**

Sécurité des matériels de traitement de l'information

- **EN50385 : (2002-08)**

Norme produit pour la démonstration de la conformité des stations de base radio et des stations terminales fixes pour les radio-télécommunications, aux restrictions de base et aux niveaux de référence relatifs à l'exposition de l'homme aux champs électromagnétiques (110 MHz à 40 GHz) Application au public en général

- **EN 300328 V1.7.1 : (2006-10)**

Compatibilité électromagnétique et spectre radioélectrique (ERM) ; systèmes de transmission de données large bande ; Équipements de transmission de données fonctionnant dans la bande ISM à 2,4 GHz et utilisant des techniques de modulation à étalement de spectre ; EN harmonisée couvrant les exigences essentielles de l'article 3.2 de la directive R&TTE

- **EN 301 893 V1.4.1 : (2007-07)**

Réseaux radio fréquence large bande (BRAN) ; réseaux locaux radio haute performance 5 GHz (RLAN) ; EN harmonisé couvrant les exigences essentielles de l'article 3.2 de la directive R&TTE

- **EN 301 489-1 V1.6.1 : (2005-09)**

Compatibilité électromagnétique et spectre radioélectrique (ERM) ; Compatibilité électromagnétique (CEM) pour standard pour les équipements de communication radio et services; Partie 1 : exigences techniques communes

- **EN 301 489-17 V1.2.1 (2002-08)**

Compatibilité électromagnétique et spectre radioélectrique (ERM) ; Compatibilité électromagnétique (CEM) pour standard pour les équipements et les services de communication radio ; Partie 17 : exigences spécifiques pour les systèmes de transmission large bande à 2,4 GHz et les équipements haute performance RLAN à 5 GHz

Cet appareil ne doit pas être utilisé pour installer des liaisons radio à l'extérieur en France, et dans certaines zones la puissance de sortie RF est susceptible d'être limitée à 10 mW EIRP dans la gamme de fréquence de 2454 MHz à 2483,5 MHz. Pour des informations détaillées, l'utilisateur final doit contacter l'Agence française de réglementation sur les télécommunications.

Cet appareil est un système de transmission large bande de 2,4 GHz (émetteur-récepteur), dont l'utilisation est autorisée dans tous les Etats membres de l'UE et de l'AELE, avec certaines restrictions d'usage en France et en Italie.

En Italie l'utilisateur final doit faire la demande d'une licence auprès des agences nationales de réglementation sur les télécommunications pour obtenir l'autorisation d'utiliser l'appareil et installer des liaisons radio en extérieur et/ou pour assurer l'accès public aux services de télécommunications et/ou de réseaux.

Annexe A : Messages du journal des échecs de connexion

Le journal de connexion (page 45) vous aide à comprendre pourquoi un périphérique ne peut pas se connecter au réseau. Cette annexe fournit des explications sur les messages du journal indiquant qu'une connexion a échoué.

Message	Raisons possibles de l'échec de la connexion
802.11: aucun point d'accès trouvé	Le point d'accès est hors de portée, désactivé ou la bande de fréquence a été modifiée.
802.11: avert.: point d'accès avec SSID trouvé, mais config. sécurité diff.	Le testeur ne dispose pas des types d'authentification/cryptage 802.1X corrects.

Message	Raisons possibles de l'échec de la connexion
échec de l'authentification	La liste de contrôle d'accès et le filtre MAC sur le point d'accès ont rejeté l'adresse MAC du testeur. Le point d'accès utilise la sécurité WEP et l'authentification 802.11 de bas niveau (ouvert/partagé) que le testeur utilise est différente du type d'authentification que le point d'accès utilise.
802.11: réception des paquet de désauthentification	Lorsqu'il suit le message 802.1X : envoi d'une clé EAP 4 canaux avec nonce client et éléments d'info , ce message est fréquemment provoqué par une touche prépartagée (expression de passe) incorrecte.
Connexion : échec attendu pendant la configuration automatique du PAC (phase 0)	Le testeur affiche toujours ce message lorsqu'il utilise l'authentification EAP-FAST pour essayer de se connecter à un point d'accès. Plusieurs phases sont nécessaires à une connexion EAP-FAST et un échec se produit habituellement pendant la phase initiale.
802.1X P2: réception d'un échec EAP	- Lorsqu'il suit le message 802.1X TLS : envoi d'un échange de clé client, ce message est fréquemment provoqué par un certificat de client incorrect. - Lorsqu'il suit le message 802.1X EAP-MSCHAPv2 : réponse au défi, il est fréquemment provoqué par un nom d'utilisateur ou un mot de passe incorrect. - Lorsqu'il suit le message 802.1X : NAK, ce message s'affiche car le serveur RADIUS ne prend pas en charge le type EAP.

Message	Raisons possibles de l'échec de la connexion
802.1X : certificat serveur non vérifié	Ignorez ce message si vous n'avez pas sélectionné l'option Vérifier le certificat du serveur dans le profil AirCheck Manager.
802.1X : le certificat serveur est erroné	L'option Vérifier le certificat du serveur a été sélectionnée dans le profil AirCheck Manager, mais le certificat chargé dans le testeur est incorrect.
DHCP : temporisation (sans le message DHCP : réussi après ce dernier)	• Le point d'accès n'a pas pu communiquer avec le serveur DHCP externe. • Le point d'accès dispose d'un serveur DHCP interne mais il est désactivé. • Le serveur DHCP a atteint ses limites pour le nombre d'utilisateurs. • Le testeur et le point d'accès sont tous deux configurés pour la sécurité WEP mais leurs paramètres clés sont différents.
DHCP : aucune offre reçue	Lorsqu'il suit le message DHCP : Temporisation , se reporter aux causes ci-dessus.
IP statique : ARP reçu. Adresse déjà utilisée	L'option Manuel (Statique) a été sélectionnée dans le profil AirCheck Manager, mais une adresse IP en double a été détectée sur le réseau.

Annexe B : Paramètres par défaut

Cette annexe présente les paramètres par défaut destinés au testeur lorsque vous sélectionnez **Outils > Restaurer aux réglages d'usine**.

Fonction	Paramètre par défaut
Profil utilisé par le testeur	Val. par défaut
Arrêt automatique	Actif
Langue	Dernière langue sélectionnée
Pays	USA
Son de la fonction de localisation du point d'accès	Actif

Fonction	Paramètre par défaut
Seuils des barres d'affichage incrémental	
Niveau de signal : Rouge	-80 dBm
Niveau de signal : Jaune	-60 dBm
Niveau de signal : Verte	-45 dBm
Niveau de bruit : Rouge	-60 dBm
Niveau de bruit : Jaune	-80 dBm
Niveau de bruit : Verte	-90 dBm
Niveau S/B : Rouge	20 dB
Niveau S/B : Jaune	30 dB
Niveau S/B : Verte	40 dB

Fonction	Paramètre par défaut
Paramètres 802.11	
Bandes	2,4 GHz et 5 GHz
Transmettre des sondages	Activer
Regrouper points d'accès virtuels	Activer
Griser points d'accès inaudibles ou Supprimer points d'accès inaudibles	Griser points d'accès inaudibles
Décalages utilisateur pour les réglages de signal personnalisés	0 dB
Liste des réseaux (SSID)	
Tri 1	SSID
Tri 2	SSID
Réseaux individuels	
Tri 1	Nom/MAC
Tri 2	Nom/MAC

Fonction	Paramètre par défaut
Points d'accès sur un canal	
Tri 1	Nom/MAC
Tri 2	Nom/MAC
Liste des points d'accès	
Tri 1	Nom/MAC
Tri 2	Nom/MAC
Liste des points d'accès virtuels	
Tri 1	SSID
Tri 2	SSID
Répertoire des clients	
Tri 1	MAC
Tri 2	Canal

Annexe C : 802.11d Codes de pays

Cette annexe indique les pays associés aux codes nationaux que le testeur affiche sur l'écran **Détails du point d'accès**.

Les pays indiqués en gras peuvent être sélectionnés dans le menu **Outils > Définir le pays**.

Remarque

Le testeur peut afficher un troisième caractère dans le code de pays. Vous pouvez ignorer ce caractère lorsque vous recherchez le code du pays dans le tableau ci-dessous.

AD	Andorre
AE	Emirats Arabes Unis
AF	Afghanistan
AG	Antigua-et-Barbuda
AI	Anguilla
AL	Albanie
AM	Arménie
AN	Antilles néerlandaises
AO	Angola
AQ	Antarctique
AR	Argentine

AS	Samoa américaines
AT	Autriche
AU	Australie
AW	Aruba
AX	Aland
AZ	Azerbaïdjan
BA	Bosnie-Herzégovine
BB	Barbade
BD	Bangladesh
BE	Belgique
BF	Burkina Faso
BG	Bulgarie
BH	Bahreïn
BI	Burundi
BJ	Bénin
BL	Saint-Barthélemy
BM	Bermudes

BN	Brunei Darussalam
BO	Bolivie
BR	Brésil
BS	Bahamas
BT	Bhoutan
BU	Birmanie (transitionnel)
BV	Bouvet (île)
BW	Botswana
BY	Bélarus
BZ	Belize
CA	Canada
CC	Cocos, îles
CD	Congo (République Démocratique du)
CF	République Centrafricaine
CG	Congo
CH	Suisse
CI	Côte d'Ivoire

CK	Cook (îles)
CL	Chili
CM	Cameroun
CN	Chine
CO	Colombie
CR	Costa Rica
CS	Serbie et Monténégro (transitionnel)
CU	Cuba
CV	Cap Vert
CX	Christmas (île)
CY	Chypre
CZ	République tchèque
DE	Allemagne
DJ	Djibouti
DK	Danemark
DM	Dominique
DO	République Dominicaine

DZ	Algérie
EC	Equateur
EE	Estonie
EG	Egypte
EH	Sahara occidental
ER	Erythrée
ES	Espagne
ET	Ethiopie
EU	Union européenne
FI	Finlande
FJ	Fidji
FK	Falkland (Malouines) (îles)
FM	Micronésie
FO	Féroé (îles)
FR	France
FX	France, métropolitaine
GA	Gabon

GB	Royaume-Uni
GD	Grenade
GE	Géorgie
GF	Guyane française
GG	Guernesey
GH	Ghana
GI	Gibraltar
GL	Groenland
GM	Gambie
GN	Guinée
GP	Guadeloupe
GQ	Guinée équatoriale
GR	Grèce
GS	Géorgie du Sud
GT	Guatemala
GU	Guam
GW	Guinée Bissau

GY	Guyane
HK	Hong-Kong
HM	Heard et McDonald (îles)
HN	Honduras
HR	Croatie
HT	Haïti
HU	Hongrie
ID	Indonésie
IE	Irlande
II	International (Cisco uniquement)
IL	Israël
IM	Île de Man
IN	Inde
IO	Territoire britannique de l'Océan Indien
IQ	Iraq
IR	Iran
IS	Islande

IT	Italie
JE	Jersey
JM	Jamaïque
JO	Jordanie
JP	Japon
KE	Kenya
KG	Kirghizstan
KH	Cambodge
KI	Kiribati
KM	Comores
KN	St Christopher et Nevis
KP	Corée, République populaire démocratique de (nord)
KR	Corée, République de (sud)
KW	Koweït
KY	Caïman (îles)
KZ	Kazakhstan

LA	Laos
LB	Liban
LC	Sainte Lucie
LI	Liechtenstein
LK	Sri Lanka
LR	Libéria
LS	Lesotho
LT	Lituanie
LU	Luxembourg
LV	Lettonie
LY	Libye (Jamahiriya arabe libyenne)
MA	Maroc
MC	Monaco
MD	Moldavie, République de
ME	Monténégro
MF	Saint Martin
MG	Madagascar

AirCheck Wi-Fi Tester

Mode d'emploi

MH	Marshall (îles)
MK	Macédoine
ML	Mali
MM	Myanmar
MN	Mongolie
MO	Macao
MP	Mariannes du Nord (îles)
MQ	Martinique
MR	Mauritanie
MS	Montserrat
MT	Malte
MU	Maurice
MV	Maldives
MW	Malawi
MX	Mexique
MY	Malaisie
MZ	Mozambique

NA	Aucun pays n'est sélectionné (situation spéciale à certains points d'accès)
NC	Nouvelle-Calédonie
NE	Niger
NF	Norfolk (île)
NG	Nigeria
NI	Nicaragua
NL	Pays-Bas
NO	Norvège
NP	Népal
NR	Nauru
NT	Zone neutre (transitionnel)
NU	Niue
NZ	Nouvelle-Zélande
OM	Oman
PA	Panama
PE	Pérou

PF	Polynésie française
PG	Papouasie-Nouvelle-Guinée
PH	Philippines
PK	Pakistan
PL	Pologne
PM	Saint Pierre et Miquelon
PN	Pitcairn
PR	Porto Rico
PS	Territoires palestiniens
PS	Etats-Unis (sécurité publique)
PT	Portugal
PW	Palaos
PY	Paraguay
QA	Qatar
RE	Réunion
RO	Roumanie
RS	Serbie

RU	Fédération de Russie
RW	Rwanda
SA	Arabie Saoudite
SB	Salomon (îles)
SC	Seychelles
SD	Soudan
SE	Suède
SF	Finlande (non officiel)
SG	Singapour
SH	Sainte Hélène
SI	Slovénie
SJ	Svalbard et Jan Mayen (îles)
SK	Slovaquie
SL	Sierra Leone
SM	San Marin
SN	Sénégal
SO	Somalie

SR	Suriname
ST	São Tomé-et-Principe
SU	URSS (ex)
SV	Salvador
SY	République arabe syrienne
SZ	Swaziland
TC	Turques-et-Caiques (îles)
TD	Tchad
TF	Territoires français du Sud
TG	Togo
TH	Thaïlande
TJ	Tadjikistan
TK	Tokelau
TL	Timor-Leste
TM	Turkménistan
TN	Tunisie
TO	Tonga

TP	Timor oriental (transitionnel)
TR	Turquie
TT	Trinité-et-Tobago
TV	Tuvalu
TW	Taïwan
TZ	Tanzanie
UA	Ukraine
UG	Ouganda
UK	Royaume-Uni (non officiel)
UM	Dépendances américaines du Pacifique
USA	Etats-Unis
UY	Uruguay
UZ	Ouzbékistan
VA	Cité du Vatican (Saint-Siège)
VC	Saint-Vincent-et-les-Grenadines
VE	Venezuela
VG	Îles Vierges (Grande-Bretagne)

VI	Îles Vierges (américaines)
VN	Vietnam
VU	Vanuatu
WF	Wallis/Futuna (îles)
WS	Samoa
YE	Yémen
YT	Mayotte
YU	Yougoslavie (transitionnel)
ZA	Afrique du Sud
ZM	Zambie
ZR	Zaïre (transitionnel)
ZW	Zimbabwe

Symboles

(...)

liste de réseaux

802.11, 26

ACL, 25

remarques, 26

sécurité, 25

liste des points d'accès

802.11, 31

ACL, 29

remarques, 31

sécurité, 30

*

Connexion, 42

nom de profil, 13, 14

point d'accès, 29

Nombres

802.11d, 20

–A–

a, 26

accessoires

en option, 68

en standard, 3

ACL, 22

activer la bande 2,4 GHz ou 5 GHz, 17

aide (coordonnées de Fluke Networks), 2

AirCheck Manager

mettre à jour le logiciel dans le testeur, 66

présentation, 1

profil, 14

transférer les fichiers vers un PC, 65

alimentation

arrêt automatique, 19

batterie, 6

ne s'éteint pas, 68

antenne

externe, 58

interne, 57

arrêt automatique, 19

assistance client, 2

—B—

b, 26

bandes de fréquence, 17

Base de connaissances, 1

batterie, 6

—C—

Caché, 26, 30, 51

canaux

bandes de fréquence, 17

détails util. canal, 40

interférence

remarque, 35

sur le graphique d'utilisation, 40

par défaut, 20

utilisation du canal, 38

certificats et conformité, 72

clients, 49

couleurs des affichages incrémentaux, 21

CURRENT.ACP, 64

—D—

date, 19

Décalages utilisateur, 61

déclaration de conformité, 75

découvrir les périphériques

clients, 49

impossible de découvrir un client, 54

impossible de découvrir un point d'accès, 34

réseaux ou points d'accès, 23

Détails du point d'accès, 32

DEVICE.XML, 64

—E—

écran d'accueil, 13

enregistrement du produit, 1

enregistrer un fichier

profil, 15

session de tests, 62

entretien, 66

état d'autorisation, 22

—F—

fichiers

ACP, 64

ACS, 64

profils, 14

renommer, 63

sessions, 62

supprimer, 63
 transférer vers un PC, 65
 XML, 64
 fichiers ACP, 64
 fichiers ACS, 64
 fichiers de session
 enregistrer, 62
 fichiers XML, 64
 Fluke Networks
 Base de connaissances, 1
 contact, 2
 flux, 37
 fonctionnalités 802.11n, 36

–G–

g, 26
 Gérer les paramètres 802.11, 17, 18
 Griser points d'accès inaudibles, 18

–H–

heure, 19
 horodatage
 liste de réseaux, 25
 liste des points d'accès, 29

–I–

icônes cadenas
 écran des points d'accès, 30, 51
 écran des réseaux, 25
 identifiants de sécurité, 14, 42
 informations sur la sécurité, 2, 66
 interférence
 remarque, 35
 sur le graphique d'utilisation, 40
 intervalle de protection, 37

–J–

journal
 écran, 45
 messages, 79

–L–

Langue, 19
 localiser un point d'accès ou un client
 utiliser l'antenne interne, 54

–M–

mémoire, 64
 mode mondial, 20
 mot de passe

profils, 14
réseau, 14

–N–

n, 26
n40+, n40–, 26
nettoyage, 66
niveaux de puissance pour la transmission, 20

–O–

options, 68

–P–

paramètres, 14
 802.11, 17
 minimum, 7
 restaurer les paramètres initiaux, 67, 83
paramètres 802.11, 17
paramètres par défaut, 83
pays, 19
 code des points d'accès, 20
 codes, 85
 paramètre, 19
périphérique ad hoc
 liste des points d'accès, 30
 liste des réseaux, 25, 30

 remarque, 35
périphérique autorisé, 22
périphérique invité, 22
périphérique non autorisé, 22
périphérique signalé, 22
périphérique voisin, 22
ping (écho)
 adresses par défaut, 44
 une adresse, 46
point d'accès virtuel, 18
points d'accès
 ACL (état d'autorisation), 22
 écran des détails, 32
 liste, 28
 localiser un point d'accès, 54, 58
 pays 802.11d, 33
 ping (écho), 46
 se connecter à un point d'accès, 42
Portée connexion, 47
profil, 14

–R–

règlement du signal personnalisé, 61
Regrouper points d'accès virtuels, 18
remarques, 35
 (...), 26, 31
réseaux

- identifiants de sécurité, 14
- liste, 25
- ping (écho), 46
- se connecter à un réseau, 42

–S–

- se connecter à un réseau ou à un point d'accès, 42
- seuils des couleurs des affichages incrémentaux, 21
- SNR, 45
- SNXXXXXX.ACS, 64
- spécifications, 69
- Supprimer points d'accès inaudibles, 18

–T–

- Témoins, 5
- touches, 5
- trames de demande de sondage
 - depuis testeur, 17
 - des clients du réseau, 49
- transférer les fichiers vers un PC, 65
- Transmettre des sondages, 17
- trier une liste, 26, 51

